ПО-16-1029
19.08.2020

ДОГОВОР

Днес,.....2020 г., в гр. София, между:

„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ" АД, ЕИК: 831641791, със седалище и адрес на управление: гр. София 1504, район „Оборище", ул. „Панайот Волов"№ 2, представлявано от Ивайло Филипов – изпълнителен директор на дружеството, в качеството му на системен интегратор по чл. 7с от Закона за електронното управление и публичен възложител на обществени поръчки по смисъла на § 45, ал. 1 от Преходните и заключителни разпоредби към Закона за изменение и допълнение на Закона за електронното управление, наричано по-долу за краткост **ВЪЗЛОЖИТЕЛ**, от една страна,

и

„КОМПЮТЪР 2000-БЪЛГАРИЯ" ЕООД, със седалище и адрес на управление гр. София, п.к. 1574, район „Слатина", ул. „Шипченски проход" № 63, Производствена сграда, ет. 4, ЕИК/БУЛСТАТ: 831816173, представлявано от Анелия Костадинова - управител, наричан по-нататък за краткост **„ИЗПЪЛНИТЕЛ"**

(**ВЪЗЛОЖИТЕЛЯТ** и **ИЗПЪЛНИТЕЛЯТ** наричани заедно „Страните", а всеки от тях поотделно „Страна")

на основание чл. 112 от Закона за обществените поръчки (ЗОП), във връзка с чл. 69 от Правилника за прилагане на Закона за обществените поръчки (ППЗОП), след проведена „открита" процедура за възлагане на обществена поръчка с предмет **„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите"**
и въз основа на Решение № 51-00-30-19/31.07.2020 г. на изпълнителния директор на „Информационно обслужване" АД за определяне на изпълнител на обществена поръчка по обособена позиция № 6 с предмет: „Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити кибер заплахи" (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*, се сключи този договор (**„Договора/Договорът"**) за възлагане на обществена поръчка.

Страните се споразумяха за следното:

Заличаването на информация в документа е на основание чл. 4 от Общ регламент за защита на данните.

I. ПРЕДМЕТ НА ДОГОВОРА

Чл. 1. (1) **ВЪЗЛОЖИТЕЛЯТ** възлага, а **ИЗПЪЛНИТЕЛЯТ** приема срещу възнаграждение да осъществи следните дейности:

1. доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричано по-нататък за краткост „оборудването" или „доставките"), подробно описано по вид, количество и технически характеристики в Техническата спецификация на **ВЪЗЛОЖИТЕЛЯ** с предмет: „Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите" – Приложение № 1 (наричана по-нататък „Техническа спецификация"), Приложение към нея, относимо към обособена позиция № 6 с предмет „Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити кибер заплахи" - Приложение № 1.6 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)* и Техническото предложение на **ИЗПЪЛНИТЕЛЯ** по обособена позиция № 6 – Приложение № 2.6 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*, представляващи неразделна част от настоящия договор.

2. гаранционно обслужване на доставеното по т. 1 оборудване (наричано алтернативно „гаранция и поддръжка"), осигурено в рамките на срока на гаранционно обслужване по чл. 4, ал. 3 в съответствие с предписанията на производителя, изискванията на настоящия договор и приложенията към него.

(2) Доставката на оборудването по ал. 1, т. 1 се извършва от **ИЗПЪЛНИТЕЛЯ** въз основа на писмена заявка до **ИЗПЪЛНИТЕЛЯ**, отправена чрез адреса за кореспонденция на хартиен носител, или по електронна поща, подписана с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис на **ВЪЗЛОЖИТЕЛЯ** или упълномощен негов представител, съгласно клаузите на този договор. В писмената заявка се посочват:

1. Вид и количество на оборудването, което следва да бъде доставено;
2. Място на доставка на оборудването;
3. Срок на доставка, съобразен със сроковете и условията на доставка по настоящия договор.
4. Друга информация по преценка на **ВЪЗЛОЖИТЕЛЯ**, относима към изпълнението на договора.

II. ЦЕНИ И НАЧИН НА ПЛАЩАНЕ

Чл. 2. (1) Общата цена по договора е в размер на 5 380 505.00 лева (пет милиона триста и осемдесет хиляди петстотин и пет лева и нула стотинки) без ДДС, съгласно Ценовото предложение на

ИЗПЪЛНИТЕЛЯ – Приложение № 3.6 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*, неразделна част от настоящия договор.

(2) **ВЪЗЛОЖИТЕЛЯТ** заплаща на **ИЗПЪЛНИТЕЛЯ** цената за изпълнената доставка съобразно цените на оборудването, посочени в Ценовото предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 3.6 към настоящия договор (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*, умножено по броя на съответното доставено и прието оборудване (хардуер и софтуер).

(3) В цените по ал. 2, съответно в общата цена по ал. 1, са включени всички разходи на **ИЗПЪЛНИТЕЛЯ** по изпълнението на договора, като **ВЪЗЛОЖИТЕЛЯТ** не дължи заплащането на каквито и да е други разноски по договора.

(4) Цените по ал. 2, съответно общата цена по ал. 1, посочени в Ценовото предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 3.6 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)* са крайни и не могат да бъдат променяни за срока на договора, освен в случаите, когато промяната е в полза на **ВЪЗЛОЖИТЕЛЯ,** както и при спазване на реда и условията на ЗОП.

Чл. 3. (1) Плащането се извършва в срок до 30 (тридесет) дни след представяне на следните документи:

1. Двустранно подписан приемо-предавателен протокол за извършена доставка по чл. 6, ал. 1; съответно чл. 6, ал. 3, когато е приложимо.

2. Оригинална фактура, предоставена от **ИЗПЪЛНИТЕЛЯ,** която съдържа подробна разбивка по единични цени, по услуги и видове за всеки един компонент, съдържащ се в доставеното оборудване.

(2) Плащането се спира, когато **ИЗПЪЛНИТЕЛЯТ** бъде уведомен, че фактурата му не може да бъде платена, тъй като сумата не е дължима поради липсващи и/или некоректни придружителни документи или наличие на доказателства, че разходът е неправомерен. В този случай, **ИЗПЪЛНИТЕЛЯТ** трябва да даде разяснения, да направи изменения или представи допълнителна информация в срок до 3 (три) работни дни, след като бъде уведомен за това. В този случай срокът за извършване на плащане към **ИЗПЪЛНИТЕЛЯ** започва да тече от датата на която **ВЪЗЛОЖИТЕЛЯТ** получи правилно оформена фактура и/или поисканите разяснения, корекции и/или допълнителна информация.

(3) Плащанията се извършват от **ВЪЗЛОЖИТЕЛЯ** в български левове, с платежно нареждане по банкова сметка, посочена от **ИЗПЪЛНИТЕЛЯ**, както следва:

Банка: Уникредит Булбанк АД

IBAN: BG96 UNCR 7630 1076 8202 47

BIC: UNCR BGSF

(4) **ИЗПЪЛНИТЕЛЯТ** е длъжен да уведомява писмено **ВЪЗЛОЖИТЕЛЯ** за всички последващи промени по ал. 3 в срок до 3 (три) дни, считано от момента на промяната. В случай че **ИЗПЪЛНИТЕЛЯТ** не уведоми **ВЪЗЛОЖИТЕЛЯ** в този срок, счита се, че плащанията са надлежно извършени.

(5) Когато **ИЗПЪЛНИТЕЛЯТ** е сключил договор/договори за подизпълнение, **ВЪЗЛОЖИТЕЛЯТ** извършва окончателно плащане към него, след като бъдат представени доказателства, че **ИЗПЪЛНИТЕЛЯТ** е заплатил на подизпълнителя/подизпълнителите за изпълнените от тях работи, които са приети по реда на раздел IV и са спазени условията на раздел IXа от настоящия договор.

III. СРОК И МЯСТО ЗА ИЗПЪЛНЕНИЕ

Чл. 4. (1) Договорът влиза в сила от датата на подписването му от двете страни и действието му се прекратява с изтичането на гаранционното обслужване, посочено в ал. 3. Датата на подписване е датата, посочена в деловодния номер на **ВЪЗЛОЖИТЕЛЯ**, поставен на стр. 1 от настоящия договор.

(2) Срокът на извършване на доставката на оборудването е до 30 (тридесет) календарни дни *(до 80 календарни дни съгласно изискванията на документацията за обществената поръчка по съответната обособена позиция)* от получаване на писмената заявка по чл. 1, ал. 2 от **ВЪЗЛОЖИТЕЛЯ**.

(3) Срокът на гаранционно обслужване на доставеното оборудване е 5 години *(минимум 5 (пет) години съгласно изискванията на документацията за обществената поръчка)* и започва да тече от датата на подписване на двустранен приемо-предавателен протокол за приемане на доставката.

Чл. 5. (1) Мястото на извършване на доставката е на територията на гр. София, като **ВЪЗЛОЖИТЕЛЯТ** ще посочи в писмената заявка по чл. 1, ал. 2 конкретния адрес на извършване на доставката.

(2) Гаранционното обслужване ще се извършва по местонахождението на доставеното и инсталирано оборудване.

IV. УСЛОВИЯ НА ДОСТАВКА. ПРЕДАВАНЕ И ПРИЕМАНЕ НА ИЗПЪЛНЕНИЕТО

Чл. 6. (1) Приемането на всяка конкретна доставка на оборудването се удостоверява с двустранен приемо-предавателен протокол, който се подписва от упълномощените представители на страните по договора. При извършване на доставка на софтуер, **ИЗПЪЛНИТЕЛЯТ** представя на **ВЪЗЛОЖИТЕЛЯ** необходимите сертификати или други документи, удостоверяващи предоставеното право на ползване на софтуера. („**Приемо-предавателен протокол за доставка на оборудването**").

(2) **ВЪЗЛОЖИТЕЛЯТ** е длъжен да прегледа доставеното оборудване в момента на доставката и незабавно да уведоми **ИЗПЪЛНИТЕЛЯ** за несъответствия по отношение на количеството и качеството на някое от доставеното оборудване, в противен случай се счита, че същите са предадени без недостатъци. Приемането на доставката на оборудването с приемо-предавателен протокол няма отношение към установените впоследствие в срока на гаранционно обслужване дефекти и/или

несъответствия, които **ИЗПЪЛНИТЕЛЯТ** е длъжен да отстрани за своя сметка в съответствие с условията на настоящия договор.

(3) При констатиране на явни недостатъци, повреди, дефекти, липси, и/или несъответствия на оборудването с Техническата спецификация – Приложение № 1, Приложение № 1.6 към нея (*попълва се за съответната позиция, за която участникът е избран за изпълнител)* или Техническото предложение – Приложение № 2.6 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)* при извършване на прегледа по ал. 2, **ВЪЗЛОЖИТЕЛЯТ** има право да откаже да подпише съответния приемо-предавателен протокол. В тези случаи страните подписват двустранен констативен протокол, в който се описват констатираните недостатъци, повреди, дефекти, липси и/или несъответствия и се посочва срокът, в който същите да бъдат отстранени (**„Констативен протокол за липса на съответствие“**). След отстраняването им страните подписват двустранен приемо-предавателен протокол по реда и условията на ал. 1 за приемане на доставката.

(4) Правилото по ал. 2 не се прилага за недостатъци, които не са могли да бъдат забелязани при обикновен преглед. В тези случаи правата на **ВЪЗЛОЖИТЕЛЯ** по ал. 3 се запазват, ако той незабавно уведоми **ИЗПЪЛНИТЕЛЯ** за откритие недостатък.

(5) Собствеността на доставеното оборудване и всички рискове преминават върху **ВЪЗЛОЖИТЕЛЯ** от датата на подписване на двустранния приемо-предавателен протокол по ал. 1 за приемане на доставката, съответно от датата на подписване на приемо-предавателния протокол по ал. 3, когато е приложимо.

(6) Когато **ИЗПЪЛНИТЕЛЯТ** е сключил договор/договори за подизпълнение, работата на подизпълнителя/подизпълнителите се приема от **ВЪЗЛОЖИТЕЛЯ** в присъствието на **ИЗПЪЛНИТЕЛЯ** и подизпълнителя/подизпълнителите.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА СТРАНИТЕ ПО ДОГОВОРА

Чл. 7. Изброяването на конкретни права и задължения на страните в този раздел от договора е неизчерпателно и не засяга действието на други клаузи от договора или от приложимото право, предвиждащи права и/или задължения на която и да е от страните.

Чл. 8. **ВЪЗЛОЖИТЕЛЯТ** има право да:

1. изисква от **ИЗПЪЛНИТЕЛЯ** да получи оборудването съгласно условията на настоящия договор и приложенията към него;

2. извършва проверка във всеки момент от изпълнението на договора относно качество, количества, стадий на изпълнение, технически параметри без с това да пречи на оперативната дейност на **ИЗПЪЛНИТЕЛЯ**;

3. изисква от **ИЗПЪЛНИТЕЛЯ** да сключи и да му представи договори за подизпълнение с посочените в офертата му подизпълнители.

Чл. 9. ВЪЗЛОЖИТЕЛЯТ е длъжен да:

1. оказва необходимото съдействие на **ИЗПЪЛНИТЕЛЯ** за изпълнение на задълженията, произтичащи от договора;

2. приеме доставеното оборудване при качествено и точно изпълнение на задълженията от страна на **ИЗПЪЛНИТЕЛЯ**;

3. да използва оборудването съобразно предназначението му и предписанията на производителя;

4. да заплати цената при извършване на доставката при качествено и точно изпълнение на задълженията, съгласно клаузите на настоящия договор.

Чл. 10. ИЗПЪЛНИТЕЛЯТ има право:

1. при пълно, точно и навременно изпълнение на задълженията си да получи уговореното възнаграждение при условията и в сроковете, посочени в настоящия договор;

2. да иска от **ВЪЗЛОЖИТЕЛЯ** необходимото съдействие за осъществяване на задълженията си по договора;

3. да иска от **ВЪЗЛОЖИТЕЛЯ** приемане на доставката, когато тя отговаря на изискванията, посочени в настоящия договор и приложенията към него.

Чл. 11. ИЗПЪЛНИТЕЛЯТ е длъжен да:

1. изпълни поръчката, предмет на настоящия договор, в срок и качествено, в съответствие с изискванията на Техническата спецификация и Техническото предложение, които представляват неразделна част от настоящия договор;

2. информира текущо **ВЪЗЛОЖИТЕЛЯ** за хода на изпълнението на настоящия договор и да го уведомява за всяко възникнало събитие, което би довело до забава и/или неизпълнение на задължение по договора и да предложи мерки за неговото преодоляване;

3. да предаде оборудването на **ВЪЗЛОЖИТЕЛЯ** в състояние, отговарящо на следните изисквания:

3.1. да е ново и оригинално, опаковано в оригинална опаковка на производителя с ненарушена цялост и всички необходимо, придружено със съответната техническа документация на електронен носител;

3.2. да отговаря на всички стандарти в Република България относно ергономичност, пожарна безопасност, норми за безопасност и включване към електрическата мрежа;

4. да заменя доставеното оборудване при констатиране от **ВЪЗЛОЖИТЕЛЯ** на скрити недостатъци с ново оборудване, отговарящо на изискванията на **ВЪЗЛОЖИТЕЛЯ**, съгласно клаузите на настоящия договор. Всички разходи по замяната са за сметка на **ИЗПЪЛНИТЕЛЯ**;

5. да извършва гаранционно обслужване на оборудването съгласно предписанията на производителя, изискванията на настоящия договор и приложенията към него,

6. по отношение на доставения софтуер (когато е приложимо):

6.1. да предоставя всички нови версии на софтуерните продукти, с оказване на необходимото съдействие на **ВЪЗЛОЖИТЕЛЯ** за изтеглянето им и за работата с тях (когато е приложимо);

6.2. да предоставя информация по запитвания и заявки от страна на **ВЪЗЛОЖИТЕЛЯ** във връзка с ползването на продуктите (когато е приложимо);

6.3. да оказва висококвалифицирана специализирана помощ и съдействие за отстраняването на възникнали инциденти и проблеми (когато е приложимо);

6.4. да отстранява възникнали грешки в софтуера и своевременното да го обновява (когато е приложимо);

6.5. да осигури свободно и безпрепятствено ползване на продуктите за срока на действие на доставените за тях лицензи (когато е приложимо).

7. да уведоми незабавно **ВЪЗЛОЖИТЕЛЯ** при възникване на пречки от стопански, административен или друг характер, които могат да забавят или да направят невъзможно изпълнението на този договор, като може да поиска от **ВЪЗЛОЖИТЕЛЯ** указания и/или съдействие за отстраняването им.

VI. ГАРАНЦИЯ ЗА ИЗПЪЛНЕНИЕ

Чл. 12. (1) При подписването на този договор, **ИЗПЪЛНИТЕЛЯТ** предоставя на **ВЪЗЛОЖИТЕЛЯ** гаранция за изпълнение в размер на 1% (едно на сто) от стойността по чл. 2, ал. 1. (**„Гаранцията за изпълнение“**) или **53 805,05 лв.** (петдесет и три хиляди осемстотин и пет лева и пет стотинки).

(2) Гаранцията за изпълнение е предназначена за обезпечаване на задълженията на **ИЗПЪЛНИТЕЛЯ** по договора, както следва:

1. 50% от сумата по ал. 1 – за изпълнение на дейностите по доставка на оборудването;

2. 50 % от сумата по ал. 1 – за изпълнение на дейностите по гаранционно обслужване.

(3) **ИЗПЪЛНИТЕЛЯТ** избира формата на гаранцията в една от следните форми:

1. парична сума внесена по банковата сметка на Възложителя;

2. банкова гаранция; или

3. застраховка, която обезпечава изпълнението чрез покритие на отговорността на **ИЗПЪЛНИТЕЛЯ.**

Чл. 13. (1) В случай на изменение на договора, извършено в съответствие с този договор и приложимото право, **ИЗПЪЛНИТЕЛЯТ** се задължава да предприеме необходимите действия за

привеждане на Гаранцията за изпълнение в съответствие с изменените условия на договора, в срок до 3 (три) работни дни от подписването на допълнително споразумение за изменението.

(2) Действията за привеждане на Гаранцията за изпълнение в съответствие с изменените условия на договора могат да включват, по избор на **ИЗПЪЛНИТЕЛЯ**:

1. внасяне на допълнителна парична сума по банковата сметка на **ВЪЗЛОЖИТЕЛЯ**, при спазване на чл. 14 от договора; и/или;

2. предоставяне на документ за изменение на първоначалната банкова гаранция или нова банкова гаранция, при спазване на изискванията на чл. 15 от договора; и/или

3. предоставяне на документ за изменение на първоначалната застраховка или нова застраховка, при спазване на изискванията на чл. 16 от договора.

Чл. 14. (1) Когато гаранцията се предоставя във вид на парична сума, тя се внася по следната банкова сметка на **ВЪЗЛОЖИТЕЛЯ:**

IBAN: BG43CECB979010C7866100;

BIC: CECBBGSF

Банка: „Централна кооперативна банка" АД

(2) Всички банкови разходи, свързани с преводите на сумата са за сметка на **ИЗПЪЛНИТЕЛЯ**.

Чл. 15. (1) Когато като гаранция за изпълнение се представя банкова гаранция, **ИЗПЪЛНИТЕЛЯТ** предава на **ВЪЗЛОЖИТЕЛЯ** оригинален екземпляр на банкова гаранция, издадена в полза на **ВЪЗЛОЖИТЕЛЯ**, която трябва да отговаря на следните изисквания:

1. да бъде безусловна и неотменяема банкова гаранция във форма, предварително съгласувана с **ВЪЗЛОЖИТЕЛЯ**, и да съдържа задължение на банката-гарант да извърши плащане при първо писмено искане от **ВЪЗЛОЖИТЕЛЯ**, декларираща, че е налице неизпълнение на задължение на **ИЗПЪЛНИТЕЛЯ** или друго основание за задържане на Гаранцията за изпълнение по този договор;

2. да бъде със срок на валидност за целия срок на действие на договора, плюс 30 (тридесет) дни, като при необходимост срокът на валидност на банковата гаранция се удължава или се издава нова.

(2) Всички банкови разходи свързани с откриването и обслужването на банковата гаранция, по усвояването на средства от страна на **ВЪЗЛОЖИТЕЛЯ**, при наличието на основание за това, както и при нейното връщане са за сметка на **ИЗПЪЛНИТЕЛЯ**.

Чл. 16. (1) Когато като Гаранция за изпълнение се представя застраховка, **ИЗПЪЛНИТЕЛЯТ** предава на **ВЪЗЛОЖИТЕЛЯ** оригинален екземпляр на застрахователна полица, предварително съгласувана с **ВЪЗЛОЖИТЕЛЯ**, издадена в полза на **ВЪЗЛОЖИТЕЛЯ**, в която **ВЪЗЛОЖИТЕЛЯТ** е посочен като трето ползващо се лице (бенефициер), която трябва да отговаря на следните изисквания:

1. да обезпечава изпълнението на този договор чрез покритие на отговорността на **ИЗПЪЛНИТЕЛЯ** в определения в чл. 12, ал. 1 размер;

2. да бъде със срок на валидност за целия срок на действие на договора, плюс 30 (тридесет) дни, като при необходимост срокът на валидност на гаранцията се удължава или се издава нова.

3. Застрахователната премията по застраховката следва да е платена на сто процента (не се допуска разсрочено заплащане на застрахователната премия) и не може да бъде използвана за обезпечение на отговорността на изпълнителя по друг договор.

(2) Разходите по сключването на застрахователния договор и поддържането на валидността на застраховката за изисквания срок, както и по всяко изплащане на застрахователно обезщетение в полза на **ВЪЗЛОЖИТЕЛЯ**, при наличието на основание за това, са за сметка на **ИЗПЪЛНИТЕЛЯ**

Чл. 17. (1) **ВЪЗЛОЖИТЕЛЯТ** освобождава гаранцията за изпълнение, както следва:

1. Сумата по чл. 12, ал. 2, т. 1 се освобождава в срок до 30 (тридесет) дни след окончателното приемане на доставката, ако липсват основания за задържането от страна на **ВЪЗЛОЖИТЕЛЯ**, на каквато и да е сума по нея.

2. Сумата по чл. 12, ал. 2, т. 2 се освобождава в срок до 30 (тридесет) дни след изтичане на срока на гаранционното обслужване, посочен в чл. 4, ал. 3, в случай, че липсват основания за задържането от страна на **ВЪЗЛОЖИТЕЛЯ**, на каквато и да е сума по нея.

(2) Освобождаването на Гаранцията за изпълнение се извършва, както следва:

1. когато е във формата на парична сума – чрез превеждане на сумата по банковата сметка на **ИЗПЪЛНИТЕЛЯ**, посочена в чл. 12, ал. 1 от договора;

2. когато е във формата на банкова гаранция – чрез връщане на нейния оригинал на представител на **ИЗПЪЛНИТЕЛЯ** или упълномощено от него лице;

3. когато е във формата на застраховка – чрез връщане на оригинала на застрахователната полица/застрахователния сертификат на представител на **ИЗПЪЛНИТЕЛЯ** или упълномощено от него лице.

(3) Гаранцията или съответната част от нея не се освобождава от **ВЪЗЛОЖИТЕЛЯ**, ако в процеса на изпълнение на договора е възникнал спор между Страните относно неизпълнение на задълженията на **ИЗПЪЛНИТЕЛЯ** и въпросът е отнесен за решаване пред съд. При решаване на спора в полза на **ВЪЗЛОЖИТЕЛЯ** той може да пристъпи към усвояване на гаранциите.

Чл. 18. **ВЪЗЛОЖИТЕЛЯТ** има право да задържи съответна част и да се удовлетвори от Гаранцията за изпълнение, когато **ИЗПЪЛНИТЕЛЯТ** не изпълни някое от неговите задължения по договора, както и в случаите на лошо, частично и забавено изпълнение на което и да е задължение на **ИЗПЪЛНИТЕЛЯ**, като усвои такава част от Гаранцията за изпълнение, която съответства на уговорената в договора неустойка за съответния случай на неизпълнение.

Чл. 19. **ВЪЗЛОЖИТЕЛЯТ** има право да задържи Гаранцията за изпълнение в пълен размер, в следните случаи:

1. при пълно неизпълнение и разваляне на договора от страна на **ВЪЗЛОЖИТЕЛЯ** на това основание;

2. при прекратяване на дейността на **ИЗПЪЛНИТЕЛЯ** или при обявяването му в несъстоятелност.

Чл. 20. Във всеки случай на задържане на Гаранцията за изпълнение, **ВЪЗЛОЖИТЕЛЯТ** уведомява **ИЗПЪЛНИТЕЛЯ** за задържането и неговото основание. Задържането на Гаранцията за изпълнение изцяло или частично не изчерпва правата на **ВЪЗЛОЖИТЕЛЯ** да търси обезщетение в по-голям размер.

Чл. 21. Когато **ВЪЗЛОЖИТЕЛЯТ** се е удовлетворил от Гаранцията за изпълнение и договорът продължава да е в сила, **ИЗПЪЛНИТЕЛЯТ** се задължава в срок до 5 (пет) дни да допълни Гаранцията за изпълнение, като внесе усвоената от **ВЪЗЛОЖИТЕЛЯ** сума по сметката на **ВЪЗЛОЖИТЕЛЯ** или предостави документ за изменение на първоначалната банкова гаранция или нова банкова гаранция, съответно застраховка, така че във всеки момент от действието на договора размерът на Гаранцията за изпълнение да бъде в съответствие с чл. 12, ал. 1 от договора.

Чл. 22. **ВЪЗЛОЖИТЕЛЯТ** не дължи лихва за времето, през което средствата по Гаранцията за изпълнение са престояли при него законосъобразно.

VII. ГАРАНЦИОННО ОБСЛУЖВАНЕ

Чл. 23. (1) **ИЗПЪЛНИТЕЛЯТ** гарантира за срока, посочен в чл. 4, ал. 3, пълната функционална годност на доставеното оборудване съгласно предписанията на производителя, изискванията на настоящия договор и приложенията към него.

(2) В рамките на срока по ал. 1 **ИЗПЪЛНИТЕЛЯТ** отстранява за своя сметка всички повреди и/или несъответствия на оборудването, съответно подменя дефектирали части, устройства, модули и/или компоненти с нови съгласно предписанията на производителя, изискванията на настоящия договор и приложенията към него.

(3) В гаранционното обслужване се включва замяна на част (компонент) със скрити недостатъци с нова или на цялото устройство с ново, ако недостатъкът го прави негодно за използване по предназначението му, както и всички разходи по замяната.

Чл. 24. (1) В случай на констатиран дефект и/или несъотвествие от страна на **ВЪЗЛОЖИТЕЛЯ**, последният се задължава своевременно да уведоми **ИЗПЪЛНИТЕЛЯ** за възникналия дефект и/или несъответствие по факс, електронна поща (e-mail) или чрез регистрация в електронната система на **ИЗПЪЛНИТЕЛЯ** (**„рекламационно съобщение“**).

(2) **ИЗПЪЛНИТЕЛЯТ** е длъжен да осигури преглед на място в срок не по-късно от следващия работен ден от 9.00 ч. до 17.30 ч. след получаване на рекламационното съобщение на **ВЪЗЛОЖИТЕЛЯ** по ал. 1. След преглед на оборудването се съставя констативен протокол за вида на

повредата и/или несъответствието, работите и срока, необходими за отстраняването („**Констативен протокол за повредата**"). Констативният протокол за повредата се подписва от представители на страните по договора.

(3) **ИЗПЪЛНИТЕЛЯТ** се задължава да отстрани настъпилата повреда и/или несъотвествие и възстановяване на пълната работоспособност на оборудването. Остраняването на настъпила повреда и/или несъответствието се осъществява по местоположението на оборудването.

(4) При невъзможост за отстраняване на настъпила повреда и/или несъответствие в срок от следващите два работни дни, **ИЗПЪЛНИТЕЛЯТ** осигурява на **ВЪЗЛОЖИТЕЛЯ** оборотно оборудване, притежаващо характеристиките в Техническото предложение на **ИЗПЪЛНИТЕЛЯ**, включително нови алтернативни решения при запазване на пълната изисквана функционалност, до пълното остраняване на повреда или несъотвествие, като срока на гаранционно обслужване на оборудването в процес на поправяне, се удължава със срока, през който е траело отстраняването на повредата.

(5) В случай, че повредата и/или несъотвествието прави устройството негодно за използване по предназначението му, **ИЗПЪЛНИТЕЛЯТ** е длъжен да замени го замени с ново, с параметри гарантиращи същата или по-добра функционалност и производителност. Приемането на новото устройство е по реда на чл. 6, ал. 1 (съответно чл. 6, ал. 3, когато е приложимо). В този случай продължава да тече срока на гаранционно обслужване за съответното заменено устройство, част от оборудването, част от оборудването, считано от датата на приемането му с приемо-предавателен протокол по чл. 6, ал. 1, (съответно чл. 6, ал. 3, когато е приложимо). Всички разходи за замяната са за сметка на **ИЗПЪЛНИТЕЛЯ.**

(6) За всяка извършена дейност по гаранционно обслужване се съставя протокол, който съдържа описание на извършената дейност. Протоколът се подписва от представители на страните по договора.

Чл. 25. (1) **ИЗПЪЛНИТЕЛЯТ** се задължава да предоставя обобщен отчет за извършените дейности по гаранционно обслужване на всяко тримесечие, които се приемат от **ВЪЗЛОЖИТЕЛЯ**. В обобщените отчети се посочва най-малко следната информация: период на покритие на отчета и списък с възникналите проблеми и параметрите, при които **ИЗПЪЛНИТЕЛЯТ** е отстранил проблемите.

(2) В случай, че **ВЪЗЛОЖИТЕЛЯТ** има забележки по представения отчет по ал. 1, **ВЪЗЛОЖИТЕЛЯТ** може да откаже да го подпише. В този случай **ВЪЗЛОЖИТЕЛЯТ** уведомява писмено **ИЗПЪЛНИТЕЛЯ** и в срок до 10 (десет) работни дни от получаване на уведомлението, страните подписват констативен протокол, в който се отразяват направените забележки и се определя срок за тяхното отстраняване. В случай че **ИЗПЪЛНИТЕЛЯТ** откаже да подпише констативния протокол **ВЪЗЛОЖИТЕЛЯТ** има право сам да състави такъв протокол като съдържанието му е задължително за **ИЗПЪЛНИТЕЛЯ**. Приемането се извършва след отстраняване на забележките в установения срок с подписването на коригиран отчет.

(3) Ако забележките не бъдат отстранени в установения срок, **ВЪЗЛОЖИТЕЛЯТ** може да развали договора с едностранно уведомление, отправено до другата страна, без да дава допълнителен срок за изпълнение.

VIII. НЕУСТОЙКИ

Чл. 26. (1) При пълно неизпълнение на договора от страна на **ИЗПЪЛНИТЕЛЯ, ВЪЗЛОЖИТЕЛЯТ** усвоява предоставената гаранция за изпълнение.

(2) При забавено изпълнение на задължения по договора от страна на **ИЗПЪЛНИТЕЛЯ** в нарушение на уговорените в този договор срокове, същият заплаща на **ВЪЗЛОЖИТЕЛЯ** неустойка в размер на 0,1 % (нула цяло и една десета на сто) от сумата по чл. 2, ал. 1, за всеки просрочен ден.

(3) При забава на **ВЪЗЛОЖИТЕЛЯ** за изпълнение на задълженията му за плащане по договора, същият заплаща на **ИЗПЪЛНИТЕЛЯ** неустойка в размер на 0,1 % (нула цяло и една десета на сто) от сумата по чл. 2, ал. 1, за всеки просрочен ден, но не повече от 3 на сто (три на сто) от тази сума.

(4) При системно (три и повече пъти) неизпълнение на задълженията за сервизно обслужване в гаранционния срок, **ИЗПЪЛНИТЕЛЯТ** дължи на **ВЪЗЛОЖИТЕЛЯ**, неустойка в размер на 0.5 (нула цяло и пет десети на сто) на сто от сумата по чл. 2, ал. 1.

Чл. 27. **ВЪЗЛОЖИТЕЛЯТ** може да претендира обезщетение за нанесени вреди и пропуснати ползи по общия ред, независимо от начислените неустойки и независимо от усвояването на гаранцията за изпълнение.

IXа. ПОДИЗПЪЛНИТЕЛИ (когато е приложимо)[1]

Чл. 27а. (1) **ИЗПЪЛНИТЕЛЯТ** е длъжен в срок от три дни от сключването на договор за подизпълнение, както и на допълнително споразумение за замяна на посочен в офертата подизпълнител, да изпрати на **ВЪЗЛОЖИТЕЛЯ** копие на договора/допълнителното споразумение, заедно с доказателства, че са изпълнени условията на чл. 66, ал. 2 или ал. 14 от ЗОП.

(2) **ИЗПЪЛНИТЕЛЯТ** носи пълна отговорност за действията и/или бездействията на подизпълнителите си, като участието им при изпълнението на поръчката, не изменя или намалява задълженията на **ИЗПЪЛНИТЕЛЯ**, съгласно настоящия договор. Видът и делът на участието на подизпълнителя/те следва да бъдат същите, като посочените в офертата на **ИЗПЪЛНИТЕЛЯ.**

(3) При сключването на договор/и с подизпълнител/и, офериран/и в офертата на **ИЗПЪЛНИТЕЛЯ,** последният е длъжен да създаде условия, че:

1. приложимите клаузи на договора са задължителни за изпълнение от подизпълнителя/ите;
2. действията на подизпълнителя/ите няма да доведат пряко или косвено до неизпълнение на договора, за което **ИЗПЪЛНИТЕЛЯТ** да иска освобождаването си от отговорност;

---

[1] Изискванията и условията, предвидени в този раздел се прилагат в случаите, когато Изпълнителят е предвидил използването на подизпълнители

3. при осъществяване на правата си по настоящия договор, **ВЪЗЛОЖИТЕЛЯТ** ще може без ограничения да извършва проверка на дейността и документацията на подизпълнителя/ите;

4. подизпълнителят няма право да превъзлага една или повече от дейностите, които са включени в предмета на договора за подизпълнение.

(4) **ИЗПЪЛНИТЕЛЯТ** може да извършва замяна на посочените подизпълнители за изпълнение на договора, както и да включва нови подизпълнители в предвидените в ЗОП случаи и при предвидените в ЗОП условия.

(5) Сключването на договор с подизпълнител, който не е обявен в офертата на **ИЗПЪЛНИТЕЛЯ** и не е включен по време на изпълнение на договора по предвидения в ЗОП ред или изпълнението на дейностите по договора от лице, което не е подизпълнител, обявено в офертата на **ИЗПЪЛНИТЕЛЯ**, се счита за неизпълнение на договора и е основание за едностранно прекратяване на договора от страна на Възложителя и за усвояване на пълния размер на гаранцията за изпълнение.

(6) Независимо от използването на подизпълнители, отговорността за изпълнение на настоящия договор е на **ИЗПЪЛНИТЕЛЯ.**

Чл. 27б. (1) Когато частта от поръчката, която се изпълнява от подизпълнител, може да бъде предадена като отделен обект на **ИЗПЪЛНИТЕЛЯ** или на **ВЪЗЛОЖИТЕЛЯ**, **ВЪЗЛОЖИТЕЛЯТ** заплаща възнаграждение за тази част директно на подизпълнителя.

(2) Разплащанията по ал. 1 се осъществяват въз основа на искане, отправено от подизпълнителя до **ВЪЗЛОЖИТЕЛЯ** чрез **ИЗПЪЛНИТЕЛЯ**, който е длъжен да го предостави на **ВЪЗЛОЖИТЕЛЯ** в 15-дневен срок от получаването му.

(3) Към искането по ал. 2 **ИЗПЪЛНИТЕЛЯТ** предоставя становище, от което да е видно дали оспорва плащанията или част от тях като недължими.

(4) **ВЪЗЛОЖИТЕЛЯТ** има право да откаже плащане по ал. 2, когато искането за плащане е оспорено, до момента на отстраняване на причината за отказа.

IX. ПРЕКРАТЯВАНЕ И РАЗВАЛЯНЕ НА ДОГОВОРА

Чл. 28. (1) Настоящият договор се прекратява:

1. с изпълнение на всички задължения на страните по договора;

2. при настъпване на обективна невъзможност за изпълнение на договора, включително отмяна на изключителните права за системния интегртор за изпълнение на съответните дейности, посредством промяна в нормативната уредба.

3. при настъпване на друга невиновна невъзможност за изпълнение, непредвидено или непредотвратимо събитие от извънреден характер, възникнало след сключването на договора („непреодолима сила"), продължила повече от 45 дни;

4. при прекратяване на юридическо лице – Страна по договора без правоприемство, по смисъла на законодателството на държавата, в която съответното лице е установено;

5. при условията по чл. 5, ал. 1, т. 3 от Закона за икономическите и финансовите отношения с дружествата, регистрирани в юрисдикции с преференциален данъчен режим, контролираните от тях лица и техните действителни собственици.

(2) Настоящият договор може да бъде прекратен:

1. по взаимно съгласие на Страните, изразено в писмена форма;

2. когато за **ИЗПЪЛНИТЕЛЯ** бъде открито производство по несъстоятелност или ликвидация – по искане на **ВЪЗЛОЖИТЕЛЯ;**

Чл. 29. **ВЪЗЛОЖИТЕЛЯТ** прекратява договора в случаите по чл. 118, ал. 1 от ЗОП, без да дължи обезщетение на **ИЗПЪЛНИТЕЛЯ** за претърпени от прекратяването на Договора вреди, освен ако прекратяването е на основание чл. 118, ал. 1, т. 1 от ЗОП. (В последния случай размерът на обезщетението се определя в протокол или споразумение, подписано от Страните, а при непостигане на съгласие – по реда на клаузата за разрешаване на спорове по този договор.)

Чл. 30. (1) Всяка от страните може да развали договора при виновно неизпълнение на съществено задължение на другата страна по договора, при условията и с последиците съгласно чл. 87 и сл. от Закона за задълженията и договорите, чрез отправяне на писмено предупреждение от изправната страна до неизправната и определяне на подходящ срок за изпълнение. Разваляне на договора не се допуска, когато неизпълнената част от задължението е незначителна с оглед на интереса на изправната страна.

(2) По смисъла на този договор „виновно неизпълнение на съществено задължение на **ИЗПЪЛНИТЕЛЯ**" е:

1. когато **ИЗПЪЛНИТЕЛЯТ** забави изпълнението на задължение по настоящия договор с повече от 30 (тридесет) календарни дни;

2. при системно (три или повече пъти) неизпълнение на задълженията на **ИЗПЪЛНИТЕЛЯ** за гаранционно обслужване на оборудването и при пълно неизпълнение на задълженията на **ИЗПЪЛНИТЕЛЯ** за гаранционното оборудване;

3. когато **ИЗПЪЛНИТЕЛЯТ** използва подизпълнител, без да е декларирал това в офертата си.

Чл. 31. При предсрочно прекратяване на договора, **ВЪЗЛОЖИТЕЛЯТ** е длъжен да заплати на **ИЗПЪЛНИТЕЛЯ** реално изпълнените и приети по установения ред доставки/услуги.

X. НЕПРЕОДОЛИМА СИЛА

Чл. 32. (1) Страните се освобождават от отговорност за неизпълнение на задълженията си, когато невъзможността за изпълнение се дължи на непреодолима сила. Никоя от страните не може да се

позовава на непреодолима сила, ако е била в забава и не е информирала другата страна за възникването на непреодолима сила.

(2) Страната, засегната от непреодолима сила, е длъжна да предприеме всички разумни усилия и мерки, за да намали до минимум понесените вреди и загуби, както и да уведоми писмено другата страна незабавно при настъпване на непреодолимата сила.

(3) Докато трае непреодолимата сила, изпълнението на задължението се спира.

(4) Не може да се позовава на непреодолима сила онази страна, чиято небрежност или умишлени действия или бездействия са довели до невъзможност за изпълнение на договора.

XI. КОНФИДЕНЦИАЛНОСТ

Чл. 33. (1) Всяка от страните по този договор се задължава да пази в поверителност и да не разкрива или разпространява информация за другата страна, станала известна при или по повод изпълнението на договора (**„Конфиденциална информация"**) включително и след прекратяването на същия, неограничено във времето. Конфиденциална информация включва, без да се ограничава до: всякаква финансова, търговска, техническа или друга информация, анализи, съставени материали, изследвания, документи или други материали, свързани с бизнеса, управлението или дейността на другата Страна, от каквото и да е естество, или в каквато и да е форма, включително финансови и оперативни резултати, пазари, настоящи или потенциални клиенти, собственост, методи на работа, персонал, договори, ангажименти, правни въпроси или стратегии, продукти, процеси, свързани с документация, чертежи, спецификации, диаграми, планове, уведомления, данни , образци, модели, мостри, софтуер, софтуерни приложения, компютърни устройства или други материали или записи или друга информация, независимо дали в писмен или устен вид, или съдържаща се на компютърен диск или друго устройство. Не се смята за конфиденциална информацията, касаеща наименованието на договора, стойността и предмета на този договор, с оглед бъдещо позоваване на придобит професионален опит от **ИЗПЪЛНИТЕЛЯ**.

(2) Конфиденциална информация за целите на настоящия договор включва и :

1. съдържанието на данъчна и осигурителна информация, лични данни или друга защитена от закон или по силата на договора информация, която е станала известна при изпълнението на този договор.

2. информация, която е станала известна при изпълнението на този договор относно вътрешни правила и процедури, структура, начин на функциониране на Националната агенция за приходите (НАП) и **ВЪЗЛОЖИТЕЛЯ**, комуникации, мрежи и информационни системи на НАП и на **ВЪЗЛОЖИТЕЛЯ**, изготвени в хода на изпълнението на документи и/или всякакви други резултати от изпълнението, разработена в полза на НАП или предоставена им документация или програмен код в явен и изпълним вид във връзка с изпълнението на настоящия договор.

(3) Лични данни се обработват от Страните единствено за целите на изпълнение на договора, при стриктно спазване на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и действащата нормативна уредба.

(4) Не се счита за нарушение на задълженията за неразкриване на Конфиденциална информация, когато:

1. Информацията е станала или става публично достъпна, без нарушаване на този договор от която и да е от страните;

2. Информацията се изисква по силата на закон, приложим спрямо която и да е от страните; или

3. Предоставянето на информацията се изисква от регулаторен или друг компетентен орган и съответната страна е длъжна да изпълни такова изискване;

В случаите по точки 2 или 3 страната, която следва да предостави информацията, уведомява незабавно другата страна по договора.

(5) Задълженията на **ИЗПЪЛНИТЕЛЯ** във връзка с изискванията за конфиденциалност включват и:

1. задължение да спазва вътрешните правила за достъп и режим на работа до сградите на НАП и на **ВЪЗЛОЖИТЕЛЯ**, когато е приложимо;

2. да спазва всички процедури и изисквания на НАП за работа в информационната инфраструктура на НАП;

3. да пази в поверителност и да не разкрива или разпространява информация за другата Страна, станала му известна при или по повод изпълнението на дейностите, предмет на договора.

4. представляващите **ИЗПЪЛНИТЕЛЯ** и лицата, които имат достъп до системите на НАП е необходимо за предоставят подписани декларации за опазване на информацията по образец, утвърден от НАП при подписване на договора и при необходимост от предоставяне на достъп до системите на НАП.

(6) С изключение на случаите, посочени в ал. 4, конфиденциална информация може да бъде разкривана само след предварително писмено одобрение от другата страна, като това съгласие не може да бъде отказано безпричинно.

(7) Задълженията по опазване от нерегламентиран достъп до конфиденциална информация се отнасят до **ИЗПЪЛНИТЕЛЯ**, всички негови поделения, контролирани от него фирми и организации, всички негови служители и наети от него физически или юридически лица, в това число подизпълнители, като **ИЗПЪЛНИТЕЛЯТ** отговаря за изпълнението на тези задължения от страна на такива лица.

(8) Всяка от страните се задължава да информира другата при нарушаване на изискванията за опазване на поверителност на информацията по този договор.

(9) Задълженията, свързани с неразкриването на Конфиденциалната информация остават в сила и след прекратяване на договора, на каквото и да е основание.

XII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 34. (1) Освен ако са дефинирани изрично по друг начин в този договор, използваните в него понятия имат значението, дадено им в ЗОП, съответно в легалните дефиниции в Допълнителните разпоредби на ЗОП или, ако няма такива за някои понятия – според значението, което им се придава в основните разпоредби на ЗОП.

(2) При противоречие между различни разпоредби или условия, съдържащи се в договора и Приложенията, се прилагат следните правила:

1. специалните разпоредби имат предимство пред общите разпоредби;

2. разпоредбите на Приложенията имат предимство пред разпоредбите на Договора.

(3) В случаите, когато **ИЗПЪЛНИТЕЛЯТ** е представил Общи условия в офертата си, при възникнало противоречие между тях и клаузите на настоящия договор, с приоритет се прилагат клаузите на договора.

Чл. 35. Настоящият договор може да бъде изменян или допълван от страните при условията на чл. 116 от ЗОП.

Чл. 36. (1) Всички уведомления между Страните във връзка с този Договор се извършват в писмена форма и могат да се предават лично или чрез препоръчано писмо, по куриер, по факс, електронна поща или по телефон, което се потвърждава писмено на следните адреси:

1. За **ВЪЗЛОЖИТЕЛЯ**:

Адрес за кореспонденция: гр. София 1504, ул. „Панайот Волов" № 2

Факс: 02/ 943 66 07

e-mail: office@is-bg.net;

тел. 02/942 03 40

2. За **ИЗПЪЛНИТЕЛЯ**:

Адрес за кореспонденция: гр. София 1574, бул. "Шипченски проход" №63, Производствена сграда „Електроника", ет. 1

Факс: няма, не използваме вече факс

e-mail: [redacted]

тел: [redacted]

Лице за контакт на този телефон: Анелия Костадинова

[redacted]

[redacted]

(2) Страните упълномощават следните представители, които да проследяват и приемат изпълнението на задълженията им по настоящия договор, да осъществяват контрол по цялостното изпълнение на Договора и да подписват предвидените в Договора документи (уведомления, протоколи и др.), както следва:

1. За **ВЪЗЛОЖИТЕЛЯ**:

[redacted] - Ръководител, информационни и комуникационни технологии, Отдел „Комуникации", e-mail: [redacted] тел. [redacted]

2. За **ИЗПЪЛНИТЕЛЯ**

[redacted] – управител.

(3) За дата на получаване на уведомлението/заявката се счита:

1. датата на предаването – при лично предаване на уведомлението;

2. датата на пощенското клеймо на обратната разписка – при изпращане по пощата;

3. датата на доставка, отбелязана върху куриерската разписка – при изпращане по куриер;

4. датата, посочена в извлечението от факс устройството– при изпращане по факс;

5. датата на която уведомлението/заявката е постъпила в посочената от ИЗПЪЛНИТЕЛЯ информационна система (e-mail) – при изпращане по електронна поща.

(4) Всяка кореспонденция между Страните ще се счита за валидна, ако е изпратена на посочените по-горе адреси (в т.ч. електронни), чрез посочените по-горе средства за комуникация и на посочените лица по ал. 2. При промяна на посочените адреси, телефони и други данни за контакт, съответната Страна е длъжна да уведоми другата в писмен вид в срок до 3 (три) работни дни от настъпване на промяната. При неизпълнение на това задължение всяко уведомление ще се счита за валидно връчено, ако е изпратено на посочените по-горе адреси, чрез описаните средства за комуникация и на посочените лица за контакт.

(5) При преобразуване без прекратяване, промяна на наименованието, правноорганизационната форма, седалището, адреса на управление, предмета на дейност, срока на съществуване, органите на управление и представителство на **ИЗПЪЛНИТЕЛЯ**, същият се задължава да уведоми **ВЪЗЛОЖИТЕЛЯ** за промяната в срок до 3 (три) дни от вписването ѝ в съответния регистър.

Чл. 37. Всички спорове по този договор ще се уреждат чрез преговори между страните, а при непостигане на съгласие, ще се отнасят за решаване от компетентния съд в Република България.

Чл. 38. За всички неуредени в този договор въпроси се прилагат разпоредбите на действащото законодателство.

Неразделна част от настоящия договор са:

1. Техническа спецификация на **ВЪЗЛОЖИТЕЛЯ** – Приложение № 1;

1.1. Приложение № 1.6 – Техническа спецификация, относима към обособена позиция № 6 с предмет „Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити кибер заплахи" - Приложение № 1.6 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*

2. Техническо предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 2.6;

3. Ценовото предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 3.6.

При подписване на договора, се представиха следните документи:

1. Гаранция за изпълнение на договора;

2. Документи по чл. 112, ал. 1 от ЗОП.

Настоящият договор се състави в 2 (два) еднообразни оригинални екземпляра на български език – 1 (един) за **ВЪЗЛОЖИТЕЛЯ** и 1 (един) за **ИЗПЪЛНИТЕЛЯ**, и се подписа, както следва:

ЗА ВЪЗЛОЖИТЕЛЯ:

[redacted]

.....

Ивайло Филипов

Изпълнителен директор

[redacted]

.....

Камелия Софрониева

Главен счетоводител

ЗА ИЗПЪЛНИТЕЛЯ:

[redacted]

.....

(подпис и печат)

Анелия Костадинова

Управител

[redacted]

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

ПО ОТКРИТА ПРОЦЕДУРА ЗА ВЪЗЛАГАНЕ НА ОБЩЕСТВЕНА ПОРЪЧКА С ПРЕДМЕТ:

„ДОСТАВКА НА КОМУНИКАЦИОННО ОБОРУДВАНЕ, ХАРДУЕР И СОФТУЕР, НЕОБХОДИМИ ЗА ОБНОВЯВАНЕ НА ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ СИСТЕМИ НА НАЦИОНАЛНА АГЕНЦИЯ ЗА ПРИХОДИТЕ“

I. ПРЕДМЕТ НА ОБЩЕСТВЕНАТА ПОРЪЧКА

1. В предмета на обществената поръчка по обособени позиции №1, № 2, № 3, № 4, № 5, № 6 и № 9 се включват следните дейности:

1.1. доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричано по-нататък за краткост „оборудването“), подробно описани по вид, количество и технически характеристики в настоящата Техническата спецификация, Приложенията към нея и Техническото предложение на участника, избран за изпълнител по съответната обособена позиция.

1.2. гаранционно обслужване на доставеното по т. 1.1. оборудване, осигурено в рамките на срока на гаранционно обслужване в съответствие с предписанията на производителя, изискванията на договора за обществена поръчка и приложенията към него.

2. В предмета на обществената поръчка по обособени позиции № 7 и № 8 се включват следните дейности:

2.1. доставка на софтуер, необходим за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричано по-нататък за краткост „софтуер“ или „доставките“), подробно описан по вид, количество и технически характеристики в настоящата Техническа спецификация, Приложенията към нея и Техническото предложение на участника, избран за изпълнител по съответната обособена позиция.

2.2. гаранционно обслужване на доставения софтуер по т. 2.1 (наричано алтернативно „гаранция и поддръжка“), осигурено в рамките на срока на гаранционно обслужване в съответствие с предписанията на производителя, изискванията на договора за обществена поръчка и приложенията към него.

II. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ПОРЪЧКАТА

1. Навсякъде в техническата спецификация, където се съдържа посочване на конкретен модел, източник, процес, търговска марка, патент, тип, произход, стандарт или производство да се чете и разбира „или ЕКВИВАЛЕНТ".

Важно! *Участникът следва да докаже, че предлаганите решения удовлетворяват по еквивалентен начин изискванията, определени от техническата спецификация.*

2. Оборудването, предмет на доставката, се състои от хардуер и софтуер, които трябва да съответстват или да надвишават в техническо отношение посочените минимални изисквания в настоящата Техническа спецификация и/или приложенията към нея. За целта участникът представя към Техническото си предложение по съответната обособена позиция подробно описание на предлаганото от него оборудване/предлагания софтуер.

3. Оборудването (хардуер и софтуер), предмет на доставката, трябва да бъде фабрично ново, неупотребявано, да е в актуалните продуктови листи на производителя към датата на сключване на договора за възлагане на обществената поръчка и да не е спряно от производство.

4. Хардуерните компоненти на оборудването трябва да отговарят на всички стандарти в Република България относно ергономичност, пожарна безопасност, норми за безопасност и включване към електрическата мрежа.

5. Оборудването следва да бъде доставено в пълно работно състояние, в оригиналната опаковка на производителя с ненарушена цялост, окомплектовано с всички необходими интерфейсни и захранващи кабели, в случай, че са различни от стандартни IEC C14 - IEC C13 или IEC C20 - IEC C19. Необходимата техническа документация, като потребителски, инсталационни, конфигурационни и др. ръководства да се представят на електронен носител за всеки тип от предлаганите устройства.

6. При доставката на софтуер следва да бъдат предоставени необходимите сертификати или други документи, удостоверяващи предоставеното право на ползване на софтуера.

III. УСЛОВИЯ НА ДОСТАВКА

1. Доставката на оборудването (хардуер и софтуер) се извършва въз основа на писмена заявка, отправена чрез адреса за кореспонденция на хартиен носител или по електронна поща, подписана с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис на възложителя или упълномощен негов представител, съгласно клаузите на договора за обществена поръчка. В писмената заявка се посочват:

1.1. Вид и количество на оборудването (хардуер и софтуер), което следва да бъде доставено;

1.2. Място на доставка на оборудването (хардуер и софтуер);

1.3. Срок на доставка, съобразен със сроковете и условията на доставка по договора за обществена поръчка.

1.4. Друга информация по преценка на възложителя, относима към изпълнението на договора за обществена поръчка.

2. Приемането и предаването на изпълнението се осъществява въз основа на изискванията на договора за обществена поръчка.

IV. ГАРАНЦИЯ И ПОДДРЪЖКА. УСЛОВИЯ НА ГАРАНЦИОННО ОБСЛУЖВАНЕ

1. Участникът, избран за изпълнител, гарантира за срока, посочен в т. V.2., пълната функционална годност на доставеното оборудване/доставения софтуер съгласно предписанията на производителя, изискванията на договора за обществена поръчка по съответната обособена позиция и приложенията към него.

2. В рамките на срока по посочен в т. V.2. и в съответствие с режима на гаранционно обслужване участникът, избран за изпълнител, отстранява за своя сметка всички повреди и/или несъответствия на оборудването, съответно подменя дефектирали части, устройства, модули и/или компоненти с нови съгласно предписанията на производителя, изискванията на договора за обществена поръчка по съответната обособена позиция и приложенията към него. В гаранционното обслужване се включва замяна на част (компонент) със скрити недостатъци с нова или на цялото устройство с ново, ако недостатъкът го прави негодно за използване по предназначението му, както и всички разходи по замяната.

3. Режимът на гаранционното обслужване на хардуера е 5 дни в седмицата (от понеделник до петък), 8 часа в рамките на работното време от 9.00 ч. до 17.30 ч.

4. Времето за реакция на избрания за изпълнител участник е до следващия работен ден от уведомяването му.

* *Време за реакция е времето от момента на уведомяване от страна на Възложителя за възникнал проблем до обратна реакция (обаждане или пристигане на място) от участника, избран за изпълнител.*

5. Избраният за изпълнител участник е длъжен да осигури преглед на място в срок не по-късно от следващия работен ден от 9.00 ч. до 17.30 ч.

6. Избраният за изпълнител участник се задължава да отстрани настъпилата повреда и/или несъответствие и възстановяване на пълната работоспособност на оборудването. Отстраняването на настъпила повреда и/или несъответствието се осъществява по местоположение на оборудването.

7. При невъзможност за отстраняване на настъпила повреда и/или несъответствие в срок от следващите два работни дни, следва да бъде осигурено оборотно оборудване, притежаващо

характеристиките в Техническото предложение на участника, избран за изпълнител, включително нови алтернативни решения при запазване на пълната изисквана функционалност, до пълното отстраняване на повреда или несъответствие, като срока на гаранционно обслужване на оборудването в процес на поправяне, се удължава със срока, през който е траело отстраняването на повредата.

8. В случай, че повредата и/или несъответствието прави устройството негодно за използване по предназначението му, избраният за изпълнител участник е длъжен да го замени с ново, с параметри гарантиращи същата или по-добра функционалност и производителност.

9. За всяка извършена дейност, избраният за изпълнител участник изготвя и предоставя протокол, който съдържа описание на извършеното. Протоколът се подписва от представители на двете страни.

10.Избраният за изпълнител участник следва да предоставя обобщен отчет за извършените дейности по гаранционно обслужване на всяко тримесечие, които се приемат от възложителя. В обобщените отчети се посочва най-малко следната информация: период на покритие на отчета и списък с възникналите проблеми и параметрите, при които избраният за изпълнител участник е отстранил проблемите.

11.Всички разходи по време на гаранционното обслужване да са за сметка на избрания за изпълнител участник.

V. СРОК НА ИЗПЪЛНЕНИЕ

1. Участникът следва да предложи в офертата си срок за извършване на доставката, който не може да бъде по-дълъг от 80 календарни дни, считано от получаване на писмената заявка по т. III.1.

2. Срокът на гаранционно обслужване е минимум 5 (пет) години, считано от датата на приемо-предавателния протокол за доставка на оборудването (хардуер и софтуер). Участникът следва да посочи в офертата си срок на гаранционно обслужване, който да отговаря на съответните изисквания.

VI. МЯСТО НА ИЗПЪЛНЕНИЕ

1. Мястото на извършване на доставката е на територията на гр. София, като конкретния адрес на извършване на доставката ще бъде посочен в писмената заявка по т. III.1. .

2. Гаранционното обслужване ще се извършва спрямо местонахождението на доставеното и инсталирано оборудване.

VII. ДРУГИ ИЗИСКВАНИЯ. ДОКУМЕНТИ КЪМ ОФЕРТАТА НА УЧАСТНИКА

1. В случай, че не е производител участникът следва да е упълномощен от производителя или от официален представител на производителя за доставка и гаранционно обслужване на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на територията на Република България.

За удостоверяване на горното участникът следва да представи Официално оторизационно писмо (или еквивалентен документ) с актуална дата от производителя или от официален представител на производителя на предлаганото оборудване. Горепосоченият документ се представя в техническото предложение на участника.

Забележка: *В случаите на представяне от участника на оторизационно писмо от официален представител на производителя, в офертата се прилага и оторизационно писмо, издадено от производителя (или еквивалентен документ), с което се упълномощава официалния представител на производителя за доставка и гаранционно обслужване на предлаганото оборудване.*

2. Участникът следва да представи Общи условия или други приложими условия за гаранционно обслужване от производителя на продуктите, предмет на обществената поръчка, като ги приложи към техническото си предложение по съответната обособена позиция, в случай, че е приложимо.

VIII. ПРИЛОЖЕНИЯ:

1. Техническа спецификация по обособена позиция № 1 с предмет: **„Доставка на централен процесорен блок за обработка на информация, софтуерни пакети и операционни системи за виртуализация и сървъри за точно време "** – Приложение № 1.1.;

2. Техническа спецификация по обособена позиция № 2 с предмет: **„Доставка на софтуерно дефинирана мрежа за пренос на данни"** – Приложение № 1.2.;

3. Техническа спецификация по обособена позиция № 3 с предмет: **„Доставка на система за филтриране, проследяване и блокиране на Интернет трафик, система за управление на технически уязвимости и защитни стени за граничен слой"** – Приложение № 1.3.;

4. Техническа спецификация по обособена позиция № 4 с предмет: **„Доставка на дискови масиви за данни и хардуерни устройства и софтуерни пакети за създаване на резервни копия и възстановяване на данни"** – Приложение № 1.4.;

5. Техническа спецификация по обособена позиция № 5 с предмет: **„Доставка на софтуерни пакети и хардуерни устройства за дефиниране на опорна мрежа, мрежово оборудване за достъп до масивите за данни, защитни стени за интернет трафик и електронна поща и за локална мрежа"** – Приложение № 1.5.";

6. Техническа спецификация по обособена позиция № 6 с предмет **„Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити кибер заплахи“** – Приложение № 1.6.

7. Техническа спецификация по обособена позиция № 7 с предмет: **„Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата“** – Приложение № 1.7.;

8. Техническа спецификация по обособена позиция № 8 с предмет: **„Доставка на система за управление и контрол на електронната идентичност и достъпа до информацията“** – Приложение № 1.8.;

9. Техническа спецификация по обособена позиция № 9 с предмет: **„Доставка на хардуерни устройства и софтуерни пакети за платформа за управление на събития и сигурността на информацията“** – Приложение № 1.9.

Приложение № 1.6.

Техническа спецификация по обособена позиция № 6 с предмет:

„Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити кибер заплахи“

1. Подсистема за засичане, разследвания и защита от познати и непознати заплахи на ниво крайна точка

Общи изисквания	
REQ.1.	Брой на крайните точки: 8000
REQ.2.	Тип решение: 1 брой основен хардуер с вграден софтуер и 5-годишна поддръжка, 1 брой хардуер за DMZ с вграден софтуер и 5-годишна поддръжка, включени 8000 лицензи (софтуерни агенти) за поставяне на крайните точки, също с 5-годишна поддръжка, 5-годишен абонамент за прилежащи услуги към 8000-те агента
REQ.3.	Решението трябва да е споменато в документа на Gartner: Market Guide for Endpoint Detection and Response Solutions.
REQ.4.	Решението трябва да притежава следните сертификати: Federal Information Processing Standards (FIPS) 140-2 и Common Criteria (CC).
REQ.5.	Решението да предоставя цялостна защита за крайни точки, включително засичане и превенция на атаки, да предоставя функции за разследване и почистване (в зависимост от метода на имплементация на решението), като да се поддържат минимално следните операционни системи на крайните точки: Window (XP, 7, 8, 10, Server 2003, 2008, 2012, 2016), mac OS X и Linux (RHEL, CentOS, Ubuntu, Suse).
REQ.6.	Решението трябва да включва специализирано устройство (хардуер), което да служи за централизирано управление на инсталираните агенти по крайните точки, за да могат да се наблюдават всички защитени крайни точки за съмнително зловредно поведение и да може да се извършва централизирано разследване.
REQ.7.	Агентите на решението трябва да могат да засичат, анализират и позволяват ответна реакция на напреднали кибератаки, използващи непознати „zero-day" уязвимости, независимо дали крайните точки се намират във или извън мрежата на организацията.
REQ.8.	Комуникацията между софтуерните агенти и централизираното управление трябва да е криптирана.
REQ.9.	Агентите на крайните точки трябва да са с малък размер, с минимално влияние на производителността на системите, като да се предоставя механизъм за контролиране на какъв процент от процесорната мощ на крайните точки да се използва за анализ и превенция на атаки, така че да не се влияе на нормалната работа на потребителите.
REQ.10.	Решението трябва да предоставя минимално следните функционалности: • Корелация в реално време на индикаторите за компроментиране на ниво крайна точка. • Засичане и блокиране на exploit атаки, използвайки алгоритми за анализиране на поведението на приложенията. Засичане на ROP (Return Oriented Programming) атаки, reverse shell, heap spray, SEHOP corruption, атаки използващи Java уязвимости.

	• Засичане на зловредни файлове в реално време. • Сканиране на файлове използвайки антивирусни алгоритми с дефиниции и чрез евристичен анализ. • Сканиране на изпълними файлове чрез алгоритми за машинно обучение (machine learning). • Възможност за сортиране на информация, за да може да се потвърди наличието на дадена атака и за да може да се възпроизведе целия ѝ жизнен цикъл за анализ. • Автоматично създаване на графика с хронолигично подредени събития, довели до компроментирането на дадена крайна точка. • Възможност за изключително бързо търсене в избрани крайни точки за зададени ключови думи, MD5 / SHA1 и SHA256 суми, сложни изрази, създадени файлове в зададен интервал от време, конкретни „бисквитки“, име на DNS хост, конкретни драйвери, файлови атрибути, HTTP хедъри, IP адреси, използвани портове за мрежова комуникация и активни процеси, конкретни ключове в регистрите на операционната система, Windows събития. • Фунцкията за търсене на информация трябва да може да се използва директно от графичния интерфейс на решението, както и използвайки API интерфейс, така че да могат да се използват автоматизирани скриптове. • Да могат да се изолират заразените крайни точки директно от централизираното управление на решението (по заявка от администратор), позволявайки им комуникация само с посочени IP адреси (Endpoint containment).
REQ.11.	Решението трябва да може автоматично да събира и да предоставя информация за използвани уязвимости, процеси, домейни, регистри, файлове и мрежова активност за вдигнатите аларми. Информацията трябва да е достъпна за преглед директно от графичния интерфейс на конзолата за централизирано управление.
REQ.12.	Решението трябва да позволява извличането на файлове от системите, на които има инсталиран агент. За Windows операционни системи, решението трябва да може да извлича заключени или изтрити файлове, ако те все още не са презаписани от нова информация.
REQ.13.	Решението трябва да позволява извличането на файлове, които са записани на крайните точки в следствие на зловредна активност, директно от интерфейса за разследване на аларми на централизираното управление.
REQ.14.	Фунцкията за извличане на файлове трябва да може да се използва директно от графичния интерфейс на решението, както и изпозлвайки API интерфейс, така че да могат да се използват автоматизирани скриптове.
REQ.15.	Решението трябва да може автоматично да генерира пакети с данни от крайните точки (endpoint triage), за да се подпомогне разследването на аларми. Пакетите с данни трябва да съдържат информация за системните параметри на крайната точка, процесите, файловете, регистрите, потребителските акаунти, история на браузването.
REQ.16.	Решението трябва да позволява извличането на информация за подпомагане на разследванията, като историята на извиканите shell команди, цялото дисково пространство на

	дадена крайна точка, цялата информация от паметта на крайната точка, историята на извиканите powershell команди, списък на процесите в паметта, списък на файловете на дисковото пространство на крайната точка.
REQ.17.	Решението трябва да може да получава индикатори за компроментиране директно от производителя и от другите подсистеми за киберсигурност, както и да се позволява създаването на собствени индикатори за компроментиране от администраторите, също така да е възможна и интеграцията с външни източници на индикатори.
REQ.18.	Решението трябва да позволява наблюдението на крайни точки и засичане на вируси тип троянски кон, червеи, шпионски софтуер, adware, key logger вируси, rootkit вируси и exploit вируси, които се появяват след употребата на приложения като например Adobe Reader, Adobe Flash, Internet Explorer, Firefox, Google Chrome, Java, Microsoft Outlook, Microsoft Word, Microsoft Excel и Microsoft PowerPoint, включително да могат да се блокират и спират от агента заразените приложения.
REQ.19.	Решението трябва да може да изпраща файлове за по-нататъшен анализ към подсистема за sandbox анализ, разположена локално в структурите на организацията (on premise).
REQ.20.	Решението трябва да може да следи изпълнението на файлове, като да може да определи дали са изпълнени за първи път или пътя на изпълнение на файловете е променен. Тази информация (мета данни) трябва да може да се изпраща към решение тип SIEM чрез интеграция.
REQ.21.	Решението трябва да може да засича непознати „zero-day" атаки, като динамичния анализ на поведението на процесите трябва да работи минимално за .dll, .ocx, .sys и изпълними (.exe) файлове, като анализа да се извършва локално, без да е необходимо изпращането на проби към облачни услуги или трети OEM решения.
REQ.22.	Агентите на решението трябва да могат да записват локално събитията свързани с работата с файлове (създаване, отваряне, модифициране), с мрежовите комуникации от крайните точки, DNS заявките, достъпените URL адреси, стартираните процеси, с използваните ключове от регистрите на операционната система.
REQ.23.	Решението трябва да позволява да се изолират заразените крайни точки директно от централизираното управление на решението (по заявка от администратор), позволявайки им комуникация само с посочени IP адреси (Endpoint containment), така че да се спре разпространението на заразата по мрежата. Механизма трябва да позволява използването на различни роли на потребителите, които да правят заявки за изолиране на заразена крайна точка и които да одобряват заявките.
REQ.24.	Решението трябва да може централизирано да обновява софтуерната версия на инсталираните агенти.
REQ.25.	Решението трябва да разполага с механизми за собствена защита от спиране или рестартиране на инсталираните агенти, както и от инжектиране на нежелани процеси в тях.
REQ.26.	Решението трябва да предоставя механизъм с използване на парола, за да се предотврати премахването на инсталиран агент от неоторизирано лице.
REQ.27.	Решението трябва да разполага с добре описан API интерфейс за интегриране.

REQ.28.	Решението трябва да позволява администрация чрез уеб-базирана конзола, без да се изисква инсталирането на допълнителен софтуер за достъпването ѝ.
REQ.29.	Решението трябва да позволява използването на прокси с оторизация за свързване със сървър за обновления на софтуера и информацията за нови заплахи.
REQ.30.	Решението трябва да може да създава, съхранява и предоставя log файлове към трети решения, използвайки Syslog протокол, например за предоставяне на информация на решения от тип SIEM.
REQ.31.	Решението трябва да позволява интеграция с решения тип SIEM за автоматична подмяна на заявки и информация, така че да се намали необходимото време за разследване на атака.
REQ.32.	В случаите когато агента не може да установи комуникация с устройството-контролер, агента трябва да продължи нормалната си работа и да изпрати събраната информация към контролера, когато комуникацията се установи отново.
REQ.33.	Решението трябва да може да се интегрира с подсистемата за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения за корелация на събития през подсистемата за централизирано управление.
Хардуерни изисквания – 2 броя основен и DMZ	
REQ.34.	Устройството да може да управлява сигурността на до 100 000 крайни точки (максимален капацитет на скалируемост)
REQ.35.	Устройството да е с максимална големина 1U
REQ.36.	Устройството да разполага с ефективно място за съхранение на получените данни от крайните точки, минимално 8TB
REQ.37.	Устройството да разполага минимално със следните портове: 2x 1GigE BaseT, 1x IPMI, 2x USB3 (rear), 1x DB9 Serial, 1x VGA
REQ.38.	Резервирано захранване – 1+1
REQ.39.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
Гаранция и поддръжка:	
REQ.40.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.41.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.42.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.43.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.

2. Подсистема за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения

Общи изисквания	
REQ.44.	Брой пощенски кутии: 8000
REQ.45.	Тип решение: 2 броя хардуер (High-Availability) с вграден софтуер и 5-годишна поддръжка, както и включен абонамент за 8000 софтуерни лицензи за анализиране на прикачени файлове и URL

	адреси в email съобщенията, също с 5-годишна поддръжка, 2 бр. 5-годишен абонамент за прилежащи услуги към хардуерните устройства
REQ.46.	Решението трябва да може да открива и идентифицира зловреден код, който е скрит и влиза в организацията чрез електронната поща, като трябва да се използват технологии и методи за засичане, които да не са базирани само на статичен анализ чрез дефиниции, статични списъци или правила, а да може да извършва и динамичен анализ и да открива непознати "zero-day" заплахи.
REQ.47.	Решението трябва да се предоставя под формата на специализиран хардуер, като производителя трябва да е отговорен и да предостави лицензи за софтуер за поне 120 виртуални машини за анализ, с прилежащите им операционни системи и приложения.
REQ.48.	Решението трябва да притежава следните сертификати: Federal Information Processing Standards (FIPS) 140-2 и Common Criteria (CC).
REQ.49.	Решението трябва да може да открива фишинг и spear-фишинг атаки. Трябва да може да анализира прикачени файлове и URL адреси в електронните съобщения, за да открива опити за компроментиране на системите на организацията.
REQ.50.	Решението трябва да може да открива impersonation атаки (представяне с чужда самоличност). Трябва да се позволява конфигурирането на отношения между имена и email адреси, така че да се засичат опити за impersonation атаки, които копират имената или email адресите на потребителите.
REQ.51.	Решението трябва да може да засича зловреден код с голяма точност, с изключително малък процент на грешни показания. Трябва да може да се открива с точност зловреден код, независимо от MIME тип, тип на разширение (extension) и независимо дали са използвани техники за скриване или архивиране на съдържанието на електронните съобщения.
REQ.52.	Решението трябва да може да поставя в карантина email съобщения, които съдържат URL адреси в тялото си, съдържат MS Office документи, PDF документи, архиви и HTML файлове, замаскирани JAVA скриптове, замаскирани, съкратени или пренасочващи URL адреси.
REQ.53.	Решението трябва да може да разпознава заплахи като извършва локален анализ, без да е необходимо да изпраща файлове, проби от зловреден код или изпълним код извън организацията или към облачно-базирани платформи за анализ.
REQ.54.	Решението трябва да може да анализира множество типове файлове, използвайки различни приложения и техни версии за анализа, съответно за разширения (минимално): exe, dll, pdf, pub, doc, docx, xls, xlsx, js, gif, jpeg, png, tiff, swf, eml, mov, qt, mp4, jpg, mp3, asf, ico, htm, hta, url, rm, com, vcf, ppt, rtf, chm, hlp.
REQ.55.	Решението трябва да може да извлича и анализира вмъкнати файлове в документи, като например pdf, rtf или MS Office документи.
REQ.56.	Решението трябва да може да поставя в карантина и да алармира за криптирани MS Office документи.
REQ.57.	Решението трябва да може да поставя в карантина и да алармира за прикачени MS Office документи, които съдържат макроси или имат вградени в тях документи, независимо от резултата от анализа.

REQ.58.	Решението трябва да може да поставя в карантина и да алармира за електронни съобщения, които съдържат в себе си съкратени URL адреси.
REQ.59.	За електронни съобщения, които съдържат URL адреси, които водят до сваляне на файлове, решението трябва да може да извлича и анализира въпросните файлове от URL адресите, като да може да се блокира съобщението ако файловете се окажат зловредни.
REQ.60.	Решението трябва да може да поставя в карантина и да алармира за електронни съобщения, които съдържат прикачени JAR файлове или съдържат URL адреси, които водят до JAR файлове.
REQ.61.	Решението трябва да може да извлича и анализира URL адреси от съдържанието на електронните съобщения и от секцията „Относно“ на съобщенията, както и от прикачени PDF или MS Office документи.
REQ.62.	Решението трябва да може да засича следните техники, които се използват от атакуващите хакери, за да подмамят потребителите да достъпят конкретни URL адреси: заместване на знак от адреса с друг (typosquatting), използване на линк към различен адрес от изображения (URL overlay).
REQ.63.	Решението трябва да може да анализира URL адреси от тип ftp, http и https.
REQ.64.	Решението трябва да може да анализира base64 кодирани URL адреси.
REQ.65.	Решението трябва да анализира прикачени архиви тип 7Z, ZIP, LZH, RAR. Ако архивите са защитени с парола, решението да може автоматично да търси подходящи варианти за парола в съдържанието на електронното съобщение, в самите файлове-архиви или в прикачени изображения към съобщението чрез OCR технология.
REQ.66.	Решението трябва да може да извлича и анализира URL адреси от заключени с парола PDF или MS Office документи. Решението да може автоматично да търси подходящи варианти за парола в съдържанието на електронното съобщение или в прикачени изображения към съобщението чрез OCR технология (изображения тип JPEG, PNG, BMP, TIFF).
REQ.67.	Решението трябва да може да анализира файлове не само чрез статичен анализ с дефиниции, но и чрез алгоритми за машинно обучение и динамичен анализ тип sandbox.
REQ.68.	Решението трябва да може да анализира (във виртуалните машини за динамичен анализ) свалените файлове от заявки идващи от exploit атаки. Например, ако прикачен файл към електронно съобщение съдържа скрипт / макрос, който опитва да свали допълнителни файлове и съдържание, то решението трябва да може успешно да ги свали и анализира, за да се открият и предотвратят атаки, които се развиват на няколко фази.
REQ.69.	Решението трябва да може да открива с много висока точност, с възможно най-малко грешни показания, файлове, които след анализ на поведението се държат по подобие на зловреден код: поведение, което опитва да избегне засичане, инсталиране на нежелани програми, промени по системните настройки, намаляване на цялостната производителност на системата, потенциално нежелани програми (PUP), потенциално нежелани приложения (PUA), adware процеси, инструменти, които често се използват от атакуващи хакери.
REQ.70.	По време на анализа във виртуалните машини, решението трябва да може да извлича и анализира URL адресите в паметта на машините.

REQ.71.	Решението трябва да може да засича ransomware криптиращи атаки и атаки предназначени за POS терминали.
REQ.72.	Решението трябва да може да алармира за зловредни процеси (файлове и URL адреси), които не са били засечени в първоначалните 24 часа, а на по-късен етап е установено, че са зловредни.
REQ.73.	Решението трябва да предоставя цялостна информация след анализ на зловреден код. Информацията трябва да включва използвани уеб линкове за атаката, хеш суми на свалените файлове, цялостен одит на действията по системите (променени ключове от регистрите, създаване и изпълнение на файлове, промяна в автоматичните настройки и параметрите за стартиране на приложения), както и да се предоставя информация за хронолигчния ред от събития, свързани с атаката, започващи от фазата на уеб-експлоатация и първоначално проникване, до свалянето на код, установяване на контрол над системите и опитите за извличане на данни извън организацията.
REQ.74.	Решението трябва да предоставя следствена информация след динамичния анализ на файлове, представена в графичен вид, изобразявайки процеси, достъпи до паметта, промени по файлове и регистри, качени DLL библиотеки, инжектиране на код, heap spraying процеси, mutex процеси.
REQ.75.	Решението трябва да може да предоставя, където е възможно, информация за атакуващата хакерска групировка и възможни стъпки за отстраняване на щетите (remediation) след дадена атака.
REQ.76.	Ако при анализ на зловреден прикачен файл се установят опити за мрежови свързвания извън организацията от него, решението трябва да сигнализира и за тях при вдигането на съответната аларма.
REQ.77.	Решението трябва да може да предоставя screenshot на зареден в браузър зловреден URL адрес по време на анализа му, за да се добие визуална представа за съдържанието на URL адреса.
REQ.78.	Решението трябва да може да прави корелация на електронни съобщения със сходни характеристики, като например с еднакви прикачени файлове, еднакви заглавни части, еднакви изпращачи и т.н. и да може да ги групира като email кампании.
REQ.79.	Решението трябва да може да прави анализ на входящи електронни съобщения, използвайки едновременно множество виртуални машини с различни операционни системи, като например минимално Windows XP, 7 или Mac OSX, с различни версии на Service Pack, на 32 и на 64 битови платформи.
REQ.80.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н. Решението трябва да използва собствен, специално изграден хипервайзор.
REQ.81.	Решението трябва да позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите трябва да могат да променят поне следните параметри: използвани потребителско име, домейн, име на работната станция,

	историята от браузването, използваният Outlook акаунт, езика на машината, времевата зона на машината.
REQ.82.	Решението трябва да може да засича опити за използване на функциите за приспиване (sleep) на операционните системи от зловредния код и да може да забързва времето на виртуалните машини за анализ, за да принуди изпълнението на зловредния код.
REQ.83.	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques), например използване на ping команди, проверка на домейн, проверка на отметки в наличните браузъри.
REQ.84.	Email решението трябва да поддържа inline MTA режим на работа.
REQ.85.	Email решението трябва да поддържа SPAN/TAP режим на работа.
REQ.86.	Email решението трябва да поддържа BCC режим на работа.
REQ.87.	Решението трябва да позволява (по избор от администратор) извършване на динамичен анализ на файлове във виртуалните машини, както в режим на изолация (без да е необходима свързаност с Интернет), така и с позволено мрежово свързване от виртуалните машини, за да се добие цялостен анализ на зловредния код.
REQ.88.	Решението трябва да използва специално заделен мрежови интерфейс когато е пуснато в „жив“ режим, за да се избегне допускането на зловреден мрежови трафик към реалната вътрешна мрежа на организацията; Мрежовия интерфейс трябва да позволява на зловредния код да достъпва външни хакерски командни сървъри и да сваля всички допълнителни модули и артефакти, които са му необходими, за да се изпълни изцяло за анализ.
REQ.89.	Решението трябва да може да симулира потребителски действия, за да изпълни зловреден код изискващ подобни действия, като например щракане с мишката или конфигуриране на конкретни данни.
REQ.90.	Цялостния анализ на електронно съобщение не трябва да отнема повече от 10 минути.
REQ.91.	Решението трябва да позволява на администраторите да конфигурират максималното време за анализ на електронните съобщения.
REQ.92.	Решението трябва да позволява използването на YARA правила и да позволява конфигурирането на автоматични аларми или поставяне в карантина ако дадено съобщение отговаря на зададените YARA правила.
REQ.93.	Решението трябва да може да засича и отчита опити за мрежова комуникация с Интернет от виртуалните машини по време на анализа.
REQ.94.	Решението трябва да позволява на администраторите да посочват и обвързват с кои приложения да се стартират различните файлови разширения по време на анализа във виртуалните машини.
REQ.95.	Решението трябва да може да се имплементира в различни режими, както „Inline”, на пътя на трафика, с възможност за блокиране, така и „Out-Of-Band“, където да се анализират копия на електронните съобщения.
REQ.96.	Решението трябва да може да работи в напълно изолирана среда, без връзка с Интернет.
REQ.97.	Решението трябва да може да изпраща автоматични известия чрез Syslog, HTTP, SNMP и SMTP протоколи.

REQ.98.	Решението трябва да поддържа криптирана TLS комуникация (opportunistic или imposed), за да се запази конфиденциалността на електронните съобщения.
REQ.99.	Решението трябва да може да изпраща автоматични известия когато блокира или постави в карантина дадено електронно email съобщение.
REQ.100.	Решението трябва да позволява конфигурирането на обема на заделеното място за карантина на съобщенията и да може да изпраща автоматични известия когато заделеното пространство се запълни до определен процент.
REQ.101.	Решението трябва да позволява използването на прокси с оторизация за свързване със сървър за обновления на софтуера и информацията за нови заплахи.
REQ.102.	Решението трябва да позволява администрация чрез уеб-базирана конзола, без да се изисква инсталирането на допълнителен софтуер за достъпването ѝ.
REQ.103.	Решението трябва да позволява конфигурирането на ACL списъци, за да се ограничи достъпа до интерфейса за централизирано управление.
REQ.104.	Решението трябва да използва криптирана комуникация между администраторите и конзолата за централизирано управление. Трябва да позволява вмъкването на собствени дигитални сертификати на организацията.
REQ.105.	Решението трябва да позволява локално конфигуриране или чрез синхронизация с NTP сървър на използваните време и часова зона.
REQ.106.	Решението трябва да поддържа ролево-базиран достъп до конзолата за управление. Да могат да се задават различни профили и права (администратор, оператор, одитор и т.н.), като да се задават кои отчети, аларми и информация могат да виждат в конзолата за управление.
REQ.107.	Решението трябва да поддържа LDAP, TACACS + или RADIUS методи за вписване на потребителите.
REQ.108.	Решението трябва да може да изпраща известия за собственото си здраве и процеси и генерираните отчети, чрез SMTP, SNMP и Syslog протоколи.
REQ.109.	Решението трябва да позволява извличането на аларми и отчети за активност на зловреден код в PDF формат.
REQ.110.	Решението трябва да позволява групирането на аларми за зловредни email съобщения по поне следните критерии: по изпращачи, по получатели, по видове вдигнати аларми, по email кампания.
REQ.111.	Решението трябва да позволява генерирането на отчети в PDF или в CSV формат, според типа информация в тях: вдигнати аларми и техните детайли, тип инфекция, обобщителна информация за предоставяне пред ръководните органи на организацията, списък с достъпените сървъри при callback комуникация и други.
REQ.112.	Решението трябва да предоставя опция да получава и изпраща обекти за анализ, когато бъде достигнат зададен лимит на капацитета на обработваните обекти от решението, към предварително зададен локално-разположен клъстър или към специализирани хардуерни устройства за балансиране на производителността.

REQ.113.	Решението трябва да позволява извличането на метаданни от email съобщенията, минимално получател, прикачени файлове и вмъкнати URL адреси, като тези метаданни да могат да се изпращат към решение тип SIEM, чрез HTTP или чрез Rsyslog протокол.
Хардуерни изисквания – 2 броя	
REQ.114.	Устройството да може да анализира до 2650 уникални прикачени файлове към email съобщения в час
REQ.115.	Устройството да може да анализира прикачени файлове и URL адреси в email съобщенията за 8000 пощенски кутии
REQ.116.	Устройството да е с максимална големина 2RU
REQ.117.	Устройството да разполага минимално със следните портове за наблюдение на мрежата: 2x 1GigE BaseT
REQ.118.	Допълнителни портове: 2x 1GigE BaseT портове за управление, сериен порт, 4x Type A USB, IPMI, VGA
REQ.119.	Резервирано захранване – 1+1
REQ.120.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
Гаранция и поддръжка:	
REQ.121.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.122.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.123.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.124.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.

3. **Подсистема за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво**

Общи изисквания	
REQ.125.	Тип решение: 2 броя хардуер (High-Availability) с вграден софтуер и 5-годишна поддръжка, с добавени 2 броя разширителни модули тип 1G-10G BASE-LX/LR FIBER, 2 бр. 5-годишен абонамент за прилежащи услуги към хардуерните устройства
REQ.126.	Предложеното решение трябва да може да инспектира и блокира зловреден мрежови трафик като да се поставя на пътя на трафика в inline режим или в „out-of-band" режим, като да може да работи независимо от останалото мрежово оборудване в инфраструктурата.
REQ.127.	Решението трябва да притежава следните сертификати: Federal Information Processing Standards (FIPS) 140-2 и Common Criteria (CC).
REQ.128.	Решението да поддържа режим на работа с висока достъпност - high availability (HA), от типа active-active.
REQ.129.	Решението трябва да може да функционира независимо от което и да е друго мрежово устройство (например защитни стени, IDS/IPS устройства, security gateway устройства и т.н.). Решението трябва да е специализирано и да може да работи самостоятелно, като функциите му не трябва да са част от UTM или интегрирано решение за сигурност.

REQ.130.	Предложеното решение трябва да предоставя предварително зададени правила за разпознаване на зловредни мрежови действия от приложенията, разположени по работните станции и сървърите в инфраструктурата на организацията. Трябва да има възможност за обновяване на тези правила използвайки актуална информация събрана от вендора за най-новите заплахи.
REQ.131.	Решението трябва да може да анализира мрежови трафик от организацията към Интернет и да засича изпълнението на нежелани приложения или callback комуникации с хакерски командни центрове, като по тази начин да могат да се блокират опити за изнасяне на информация извън организацията по мрежата, като или да се блокира мрежовата сесия ако се работи в inline режим или като вгражда „reset" пакети в комуникацията ако се работи в „out-of-band" режим.
REQ.132.	Решението да може да функционира като ICAP сървър, като да може да получава файлове за анализ чрез ICAP протокола.
REQ.133.	Решението трябва да може да засича ранните фази на уеб-базираните атаки, например първоначално стартиране на exploit, сваляне на зловреден бинарен код, callback функции и комуникации с хакерски командни центрове, за да може да идентифицира уязвимости в системите и приложенията на организацията, за да може да засича заразени системи и за да може да блокира неоторизирани комуникации навън от средата, по няколко мрежови протокола.
REQ.134.	Предложеното решение трябва да може да инспектира и да открива зловредни обекти, зловредни URL мрежови адреси и зловредни действия в поне следните мрежови протоколи: HTTP, HTTPS, FTP, SMB.
REQ.135.	Предложеното решение трябва да може да засича движение на атаките „настрани" в организацията (lateral spread) като анализира SMB, WinRM и MS-SQL трафик и да може да засича и алармира за дейности след успешен exploit на уязвимости от атакуващите, от вътрешна работна станция до вътрешен трафик (трафик тип изток-запад), като например вътрешно разузнаване, ескалиране на права за достъп на акаунти, извличане на потребителски имена и пароли, движение „настрани" на зловреден код, изпълнение на дистанционни команди, извличане на данни.
REQ.136.	Предложеното решение трябва да е под формата на специализирано хардуерно устройство и вендора трябва да предостави пълни лицензи за софтуера, който ще се използва от устройството за анализиране на зловреден код, както и необходимите лицензи за операционните системи и приложенията, използвани от виртуалната среда за анализ на кода.
REQ.137.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението трябва да използва собствен, специално изграден хипервайзор.
REQ.138.	Решението трябва да позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите трябва да могат да променят поне следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, използваният Outlook акаунт, езика на машината, времевата зона на машината.

REQ.139.	Решението трябва да предоставя среда за динамичен анализ, която да се състои от предварително създадени виртуални машини, които да са изцяло предоставени и поддържани от вендора на решението, за да се избегне сложността произтичаща от инсталирането на приложения и поддръжката на виртуални машини от страна на организацията.
REQ.140.	Решението трябва да може да идентифицира атаки, без да внася забавяне в мрежовия трафик на организацията, като анализа трябва да се извършва локално, на мрежовото ниво, където е разположено устройството.
REQ.141.	Решението трябва да има механизъм за класифициране и поставяне на етикети на бинарен код на машинно ниво, които се отнася за EXE, DLL и SYS файлове.
REQ.142.	Предложеното решение трябва да дава възможно най-малко грешни показания и да вдига възможно най-малко грешни аларми при засичането на файлове, които наподобяват зловреден код: да алармира за поведение, което опитва да избегне засичане от системите за сигурност, инсталиране на нежелани програми, промяна на системните настройки, което влошава производителността на системите, наличие на потенциално нежелани програми (PUP) и на потенциално нежелани приложения (PUA), adware процеси и използване на инструменти, които често се използват от атакуващи хакери.
REQ.143.	Решението трябва да може да разпознава заплахи чрез извършване на локален анализ, без да се изпращат файлове, проби от кода или изпълним код извън организацията или към облачно-базирани системи за анализ.
REQ.144.	Трябва да има възможност за комплексно разследване за целия цикъл на атаките, включително върху всяка от следните фази, за които да има отделни аларми: • Първоначално разпознаване на мрежата (Картографиране на мрежата, преброяване на хостовете, преброяване на услугите, издирване на потребителски акаунти); • Изпълнение (използване на командата „AT“ за насрочване на изпълнение на процеси, „pass-the-hash“ дистанционно изпълнение на код (RCE), използване на инструментариума за управление на Windows средите (WMI), дистанционно създаване на процеси); • Изпълнение на Web Shell; • Сваляне на зловреден код (malware); • Извличане на информация чрез свързвания с хакерски команден сървър; • Разпространяване на зловредния код (трансфер на зловреден код чрез SMB и SMB 2 протоколи) • Ескалиране на привилегии (преброяване на групите с високо ниво на достъп, преброяване на дистанционно споделените ресурси - remote shares) • Извличане на данни за вписване в системите (трансфер на пароли чрез SMB протокол, извличане чрез Mimikatz, извличане на NTLM хешове) • Дистанционно изпълнение на процеси.
REQ.145.	Решението трябва да може да идентифицира уеб-базирани уязвимости, чрез извършване на анализ на съмнително уеб съдържание във виртуалните машини за анализ, използвайки същия тип браузър, както реалния потребител достъпил уеб съдържанието.

REQ.146.	Решението трябва да може да засича атаки към сървърите като извлича и анализира статични и динамични уеб-базирани файлове (PHP, WAR, JSP, ASP, ASPX), които са качени на уеб сървърите чрез HTTP POST или FTP.
REQ.147.	Решението трябва да предоставя детайлна информация за аларми, произлизащи от извлечените метаданни от транспортния и от приложния слой на мрежата, за поне следните протоколи: FTP, HTTP, IMAP, IRC, POP3, RDP, RTSP, SIP, SMB, SMTP, SSH, TLS; Решението трябва да може да визуализира метаданните в интерактивна, графична форма, както и да позволява извличането им за интегриране с трети SIEM решения.
REQ.148.	Решението трябва да може да инспектира HTTPS трафик, като да се поддържат SSL / TLS протоколи, включително да се поддържат функции като JA3 fingerprinting, използване на „бели списъци“ и URL категоризация.
REQ.149.	Решението трябва да може да анализира поне следните файлови типове: msi, exe, dll, pdf, doc, chm, avi, jar, docx, xls, xlsx, gif, jpeg, png, tiff, swf, swf embedded in swf, scr, mov, qt, mp4, jpg, mp3, asf, ico, htm, hta, url, rm, com, vcf, ppt, rtf, chm, hlp и други.
REQ.150.	Решението трябва да предоставя „предварителен изглед“ на засечените съмнителни URL адреси, като да може да предоставя на анализаторите screenshot-и от URL адресите.
REQ.151.	Решението трябва да може да извършва динамичен анализ за зловреден код, да може да се обновява и да може да му се предоставя нова информация за заплахи, дори в offline режим, без да има връзка с Интернет.
REQ.152.	Решението трябва да може да предоставя контекстуална информация към вдигнатите аларми, като например източник, степен на опасност, потенциални рискове, варианти за справяне с проблема и т.н., за засечените атаки от дадена рискова група.
REQ.153.	Решението трябва да разполага с голям набор от виртуални машини за sandbox анализ, с предварително инсталирани операционни системи и софтуер, бивайки Windows OS (включително XP, 7, 10), Mac OSX и Linux Cent OS, с различни версии на Service Pack, 32 и 64 битови, за да може да извършва точен анализ на поведението на процесите според различните уязвимости на средите.
REQ.154.	Решението трябва да предоставя множество приложения с различни версии за тестове, разположени на виртуалните машини за анализ на зловредни файлове. Приложенията и версиите трябва да бъдат минимум следните: Microsoft Office 2003, 2007, 2010, 2013; Adobe Reader 7, 8, 9, 10, 11; Internet explorer 6, 7, 8, 9, 10, 11.
REQ.155.	Решението трябва да може да анализира един и същ файл на различни видове и версии на операционни системи и приложения, както и на различни версии на Internet Explorer, за да се открие потенциално зловредно поведение използващо конкретни уязвимости.
REQ.156.	Решението трябва да може да алармира за зловредни процеси, които не са били засечени в първоначалните 24 часа, а на по-късен етап е установено, че са зловредни.
REQ.157.	След извършване на анализ, решението трябва да може да предоставя пълен отчет за него, който да съдържа минимално следната информация: • Тип на анализираните файлове; • Име на пробата;

	• Контролните суми на анализираните файлове (MD5, SHA1 / 256/512); • Класификация според това към кое семейство се причислява засечения зловреден код; • Тип на използваната уязвимост за пробив; • URL адреси, които са използвани за атаката, както и предоставяне на информация за преглед на съдържанието на URL адресите чрез изображения (screenshots); • Данни за идентифициране на заразените системи (IP, MAC); • Графично изобразяване на поведението на анализирания зловреден код; • Извършени промени по операционните системи; • Извършени промени по инсталираните приложения на виртуалните машини за анализ; • Извършени промени по файловата система; • Извършени промени по регистрите на Windows операционните системи; • Качените DLL библиотеки; • Извиканите Windows API функции, в хронологичен ред; • Информация за създадените / модифицираните / спрените процеси; • Детайлно изобразяване на поведението на процесите на мрежово ниво в графичен формат (изпълнени мрежови свързвания и използваните транспортни мрежови протоколи, използвани портове, DNS заявки и отговори, http пакети); • Информация за IP адресите, с които е комуникирано;
REQ.158.	Решението трябва да може да съхранява данните от изпълнението на зловреден код и прилежащите артефакти, като например PCAP файл с данни от засечените заплахи, за да може информацията да се анализира допълнително и след извършения sandbox анализ.
REQ.159.	Решението трябва да може да се поставя в следните режими на работа: SPAN, TAP, inline или HW bypass.
REQ.160.	Решението трябва да позволява използването на YARA правила.
REQ.161.	Решението трябва да може да анализира мрежови трафик независимо от използваните VLAN и портове, без да изисква предварително задаване на параметри, включително да се поддържат протоколи Encapsulated remote SPAN, Virtual Extensible LAN и Internet Content Adaptation Protocol.
REQ.162.	Решението трябва да разполага с команден и с графичен интерфейс (достъпен през стандартен уеб-браузър) за централизирано управление, без да се изисква инсталиране на допълнителен софтуер.
REQ.163.	Решението трябва да поддържа ролево-базиран достъп до конзолата за управление. Да могат да се задават различни профили и права (администратор, оператор, одитор и т.н.), като да се задават кои отчети, аларми и информация могат да виждат в конзолата за управление.
REQ.164.	Решението трябва да може да анализира и засича атаки, които протичат на няколко нива и фази, а да не предоставя само sandbox технология за анализ на отделни файлове в изолация.
REQ.165.	Решението трябва да борави с различни версии на Microsoft Office във виртуалните машини за анализ, като да може да анализира Microsoft Office документи с вграден зловреден код или макроси за пароли, анализ на зловреден трафик от тях, както и да се засичат системни грешки свързани с документите.

Приложение № 1.6.

REQ.166.

	• Мета данни от зловредния код; • Уловен мрежови трафик (PCAP файл) от виртуалните машини за анализ; • Пълно описание на достъпените URL адреси от зловредния код с идентифицирне на локациите им.
REQ.179.	Решението трябва да може да предоставя извличането на отчети и аларми в PDF формат.
REQ.180.	Решението трябва да може да определи степента на заплаха на даден инцидент от вдигнатите аларми за него.
REQ.181.	Решението трябва да може да вдига различни аларми за всяка фаза от жизнения цикъл на засечените атаки.
REQ.182.	Решението трябва да може да засича опити за използване на функциите за приспиване (sleep) на операционните системи от зловредния код и да може да забързва времето на виртуалните машини за анализ, за да принуди изпълнението на зловредния код.
REQ.183.	Решението трябва да може да симулира потребителски действия, за да изпълни зловреден код изискващ подобни действия, като например щракане с мишката или конфигуриране на конкретни данни.
REQ.184.	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques),

REQ.195.	Устройството да поддържа следните режими на работа на портовете за наблюдение на мрежата: In-line Monitor, Fail-Open, Fail- Close (HW Bypass) или TAP/SPAN
REQ.196.	Допълнителни портове: 2x 1GigE портове за управление, сериен порт, 4x Type A USB, IPMI, VGA
REQ.197.	Резервирано захранване – 1+1
REQ.198.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
Гаранция и поддръжка:	
REQ.199.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.200.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.201.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.202.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.

4. **Подсистема за централизирано управление**

Общи изисквания	
REQ.203.	Тип решение: 1 брой хардуер с вграден софтуер и 5-годишна поддръжка
REQ.204.	Решението трябва да може да извършва корелация на аларми между подсистемата за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво и подсистема за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения, както и подсистемата за засичане, разследвания и защита от познати и непознати заплахи на ниво крайна точка, за да се предостави защита от атаки, които се изпълняват на няколко нива и през няколко вектора. Например: атака чрез зловреден URL адрес, предоставен чрез

REQ.211.	Решението трябва да предоставя интегрирана централизирана администрация, в реално време, използвайки графичен интерфейс, който да предоставя следните функции: • Преглед и филтриране на събития свързани със сигурността; • Идентифициране на заразени устройства; • Централизиране на всички известия и аларми от управляваните подсистеми; • Персонализиране на графичното изобразяване на информацията (персонализиране на dashboards); • Създаване и извличане на отчети в PDF и HTML формати.
REQ.212.	Решението трябва да позволява използването и дистрибутирането на индикатори за компроментиране от трети източници (индикатори, които могат да бъдат URL адреси, IP адреси, домейни и хеш суми на зловредни файлове) към управляваните подсистеми. Индикаторите за компроментиране трябва да могат да се управляват или чрез използването на списъци за всяка категория или чрез използването на STIX (Structured Threat Information Expression) формат.
REQ.213.	Решението трябва да поддържа LDAP, TACACS + или RADIUS методи за вписване на потребителите, както и чрез Активна Директория или решения за двуфакторна автентикация.
REQ.214.	Решението трябва да може да създава, съхранява и предоставя log файлове към трети решения, използвайки Syslog протокол, например за предоставяне на информация на решения от тип SIEM.
Хардуерни изисквания – 1 брой	
REQ.215.	Устройството да е с максимална големина 2RU
REQ.216.	Устройството да разполага с поне 4TB за съхранение на данни
REQ.217.	Устройството да разполага минимално със следните портове за свързване с мрежата: 2x 1GigE BaseT
REQ.218.	Допълнителни портове: 2x 1GigE BaseT портове за управление, сериен порт, 2x Type A USB, IPMI, VGA
REQ.219.	Резервирано захранване – 1+1
REQ.220.	Устройството да може да управлява другите устройства за защита на крайни точки, за мрежова защита и за email защита, като всички те трябва да бъдат от един производител
Гаранция и поддръжка:	
REQ.221.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.222.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.223.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.224.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.

5. **Подсистема за централизирано разтоварване на процесите по извършване на динамичен анализ на зловреден код и на кибератаки от другите подсистеми за киберсигурност**

Общи изисквания

REQ.225.	Решението трябва да поддържа наблюдение чрез SNMP v3.
REQ.226.	Решението трябва да може да инициализира и използва до 192 виртуални машини едновременно за sandbox анализ, за да може да обработи голям обем от трафик.
REQ.227.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението трябва да използва собствен, специално изграден хипервайзор.
REQ.228.	Решението трябва да може да получава автоматично данни за заплахи от засечени такива при други клиенти на вендора от цял свят.
REQ.229.	Решението трябва да може да прави анализ на големи файлове до 1024 MB.
REQ.230.	Решението трябва да може да създава локални дефиниции (signatures) на засечените зловредни файлове. Администраторите трябва да могат да конфигурират времето на изтичане на валидността на локалните дефиниции.
REQ.231.	Решението трябва да позволява модифициране на параметрите на Outlook акаунта, използван в sandbox средата.
REQ.232.	Решението трябва да може да засича webshell скриптове.
REQ.233.	Решението трябва да може да изпълнява файлове създадени от MS Office документи в startup директорията на операционната система по време на sandbox анализа.
REQ.234.	Решението трябва да може да изпълнява планираните (scheduled) задачи от зловредния код в sandbox средата.
REQ.235.	Решението трябва да позволява на администраторите да конфигурират датата и часа (времевата зона) и използвания език в sandbox средата.
REQ.236.	Решението трябва да може да извлича URL адреси от паметта по време на sandbox анализа.
REQ.237.	Решението трябва да може да извлича URL адреси от Microsoft Office файлове и от XPS файлове.
REQ.238.	Решението трябва да може да извлича и анализира свързани Relationship URL адреси.
REQ.239.	Решението трябва да може да засича зловредни Microsoft Office файлове с вградено видео в тях.
REQ.240.	Решението трябва да може да извършва анализ на следните специални файлови типове: REG, Microsoft Access, One Note, HTA и Scriptlet.
REQ.241.	Решението трябва да може да анализира Microsoft Office файлове, които са защитени с парола.
REQ.242.	Решението трябва да може да засича инжектиране на код.
REQ.243.	Решението трябва да може да извършва анализ на файлове използвайки различни версии на Microsoft Office на виртуалните машини за sandbox анализ.
REQ.244.	Решението трябва да може да извлича и анализира вградени файлове в Microsoft Office файлове.
REQ.245.	Решението трябва да може да наблюдава PowerShell дейностите в sandbox средата и да може да докладва за тях.
REQ.246.	Решението трябва да може да извлича файлове, създадени от PowerShell процеси.

REQ.247.	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques) от зловредните процеси, като например PING проверки, проверки за време и техники с диалогови прозорци.
REQ.248.	Решението трябва да може да засича нови криптовируси (ransomware) в sandbox средата – без да има дефиниции (signatures) за тях.
REQ.249.	Решението трябва да поддържа Microsoft Windows 10 за засичане на drive-by атаки.
REQ.250.	Решението трябва да може да засича Point of Sale зловредни процеси.
REQ.251.	Решението трябва да може да засича зловредни процеси, използващи kernel уязвимости.
REQ.252.	Решението трябва да може да засича DDE атаки.
Хардуерни изисквания – 2 броя	
REQ.253.	Необходими са 2 броя устройства, които да могат да поемат процесите по анализиране на зловреден код, като по тази начин да може да се увеличи производителността и капацитета на работа на подсистемата за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво, както и да могат да поемат процесите по анализиране при необходимост от подсистемата за динамичен анализ на зловреден код и защита от кибератаки за мрежови файлови дялове, както и от подсистемата за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения, да може да увеличава тяхната производителност и капацитет на работа.
REQ.254.	Устройството да е с максимална големина 2RU
REQ.255.	Устройството да разполага с поне 4TB за съхранение на данни
REQ.256.	Устройството да разполага минимално със следните портове за свързване с мрежата: 1x 10/100/1000 Mbps BASE-T, 2x 10 Gbps BASE-T, 4x 10GigE SFP+
REQ.257.	Допълнителни портове: 1x 10/100/1000 Mbps BASE-T порт за управление, сериен порт, 2x Type A USB, IPMI, VGA
REQ.258.	Резервирано захранване – 1+1
REQ.259.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
Гаранция и поддръжка:	
REQ.260.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.261.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.262.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.263.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.

6. **Подсистема (лаборатория) за динамичен анализ на зловреден код**

Общи изисквания	
REQ.264.	Тип решение: 1 брой хардуер с вграден софтуер и 5-годишна поддръжка, 5-годишен абонамент за прилежащи услуги
REQ.265.	Решението трябва да предоставя на анализаторите на сигурността защитена среда, в която те да могат да тестват, стартират и документират процесите на сложни зловредни кодове

	(malware), като да се предоставят голям набор от виртуални машини, с предварително инсталирани операционни системи и софтуер, бивайки Windows OS (включително XP, 7, 10), Mac OSX и Linux Cent OS, като да могат да се стартират и използват поне 30 виртуални машини едновременно.
REQ.266.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението трябва да използва собствен, специално изграден хипервайзор.
REQ.267.	Виртуалните машини, които ще се използват за анализа, трябва да имат инсталирани най-базовите браузъри (минимално Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome, Safari), плъгини (минимално Adobe Flash) и други необходими приложения от трети разработчици (минимално Adobe Reader , VLC, QuickTime, Real Player, Microsoft Office Word, Excel, Powerpoint, Preview).
REQ.268.	Лицензите за операционните системи и за комерсиалните приложения на предварително създадените и конфигурирани виртуални машини трябва да бъдат предоставени от вендора на решението за динамичен анализ.
REQ.269.	Решението трябва да позволява автоматичното възстановяване на виртуалните машини за анализ към предварително конфигурираното им базово състояние, веднага щом приключи анализа на подадена проба от зловреден код.
REQ.270.	Решението трябва да позволява взаимодействие от анализаторите с виртуалните машини по време на динамичния анализ.
REQ.271.	Решението трябва да може да извършва анализ на поне следните файлови типове: 7zip, zip, rar, gz, 3gp, accdb, app, apk, applet, asf, asp, aspx, avi, bat, cdf, chm, cmd, com, csv , dll, dmg, doc, docx, eeml, elf, eml, exe, flv, gen, gif, hlp, hta, htm, ico, inf, inf64, jar, jpeg, jpg, js, jsp, lnk, mach-o , midi, mov, mp3, mp4, mpg, mpkg, msg, msi, one, onepkg, pdf, php, pkg, pl, png, ppsx, ppt, pptx, ps1, pub, py, pyc, qt, raw32, raw64 , rb, reg, rm, rmi, rtf, sct, sh, swf, swf built-in swf, tiff, url, url-applet, vbs, vcf, vcs, war, wav, wma, wsf, xdp, xls, xlsx, xml, xsl, shell скриптове ако са уеб-базирани (Python, Perl, Ruby), txt.
REQ.272.	Решението трябва да може да прави анализ на големи файлове до 1024 MB.
REQ.273.	Решението трябва да може да извършва статичен и динамичен анализ по поне следните методи: YARA, сканиране с антивирусни дефиниции, Python-базиран статичен анализ, засичане на dropper процеси, анализ на URL адреси, които са вградени във файлове и електронни съобщения, анализ на riskware, анализ на динамичните процеси във виртуалните машини.
REQ.274.	Решението трябва да може да анализира целия жизнен цикъл на дадена кибератака, започвайки от първоначалното проникване в системата (exploit), свързвания с хакерски команден център и сваляне на вторични зловредни модули.
REQ.275.	Решението трябва да позволява сравнението на поведението на анализирания зловреден код под различните конфигурации на средата за анализ (при различни версии на Microsoft Windows и Mac OSX операционни системи, различни версии на инсталираните приложения, различни настройки на операционните системи, при различни приложени обновления на операционните системи, при приложени различни кръпки и Service Pack версии).

REQ.276.	Предложеното решение трябва да дава възможно най-малко грешни показания и да вдига възможно най-малко грешни аларми при засичането на файлове, които наподобяват зловреден код: да алармира за поведение, което опитва да избегне засичане от системите за сигурност, инсталиране на нежелани програми, промяна на системните настройки, което влошава производителността на системите, наличие на потенциално нежелани програми (PUP) и на потенциално нежелани приложения (PUA), adware процеси и използване на инструменти, които често се използват от атакуващи хакери.
REQ.277.	Решението трябва да позволява едновременното използване на няколко виртуални машини за анализ, където различни зловредни приложения да могат да бъдат анализирани по едно и също време, без да взаимодействат помежду си.
REQ.278.	Решението трябва да може да симулира човешки действия по виртуалните машини за анализ, така че дори зловредните приложения, които имат проверки в себе си дали в момента взаимодействат с реален потребител (извиквайки някои вградени функции на Windows или от Windows API интерфейса), да се изпълнят напълно и да могат да бъдат анализирани.
REQ.279.	По време на извършване на анализа във виртуалните машини, решението трябва да може да се справя с опити от зловредния код за избягване на засичане, като например използване на ping командите, проверка на домейна, проверка на отметките в браузърите, проверка на Outlook акаунтите, проверка на активните процеси, верифициране DNS.
REQ.280.	Решението трябва да може автоматично да взаимодейства със зловредни приложения, които използват графичен интерфейс и които изискват взаимодействие с извикани диалогови прозорци или с извършване на стъпки по инсталирането на приложения.
REQ.281.	Решението трябва да позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите трябва да могат да променят поне следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, наскоро достъпени файлове, DNS записи.
REQ.282.	Решението трябва да позволява създаването на подробни технически отчети, които да съдържат информация за анализираните файлове, като например: • Типа на анализирания файл; • Контролните суми (MD5, SHA) на анализираните файлове / създадените файлове на виртуалните машини за анализ; • Проверка с YARA правила; • Инстинкия тип на анализирания файл; • MD5 и SHA1 стойности на първоначалния обект, но също и на всеки друг обект създаден от него; • Използваните DLL библиотеки, респективно функциите използвани от зловредния код, излвечени от IAT таблицата; • Датата на компилиране на файла; • Направените промени на ниво инсталираните приложения на системите за анализ; • Промени по файловата система; • Направените промени по Windows Registry базата от данни;

	• Извиканите Windows API функции, в хронологичен ред; • Информация за създадените / модифицираните / спрените процеси; • Информация за създадените / модифицираните / спрените Windows услуги (services); • Създадените Mutex обекти; • За всички създадени SSDT, IDT, IRP Hooks; • Направени мрежови свързвания и използвани транспортни мрежови протоколи; • Уловен мрежови трафик (под формата на PCAP файл), произтичащ от системата за анализ; • DNS заявки; • Достъпени IP адреси и използвани логически портове; • Уловени съмнителни процеси на виртуалната машина при анализа; • Записани screenshots / видео, направени по време на анализа на зловредните приложения; • Типа на използваните уязвимости (exploits) от зловредния код.
REQ.283.	Решението трябва да може да издава отчети в следните формати: PDF, CSV, Text, JSON, XML.
REQ.284.	Решението трябва да използва специално заделен мрежови интерфейс когато е пуснато в „жив" режим, за да се избегне допускането на зловреден мрежови трафик към реалната вътрешна мрежа на организацията; Мрежовият интерфейс трябва да позволява на зловредния код да достъпва външни хакерски командни сървъри и да сваля всички допълнителни модули и артефакти, които са му необходими, за да се изпълни изцяло за анализ, включително когато мрежата е конфигурирана да използва уеб прокси.
REQ.285.	Решението не трябва да позволява мрежови комуникации от виртуалните системи/sandbox за анализ към Интернет, когато решението е пуснато в Sandbox режим: зловредния код във виртуалните машини не трябва да може да комуникира с хакерски командни центрове или URL адреси в Интернет в този режим.
REQ.286.	Решението трябва да може да засича когато зловредния код извиква sleep функции и да поставя времева точка в бъдещето, която да отговори на условието за изпълнение. Да може да симулира човешки действия като например кликване с мишката, за да може да стартира такъв тип зловреден код, използващ такива критерии.
REQ.287.	Решението да позволява на администраторите да могат да избират с кои приложения да се стартира анализа в дадена виртуалната машина.
REQ.288.	Решението трябва да може да разпознава зловредно поведение от общ характер, както и да класифицира зловредните приложения от дадено семейство вируси (троянски кон, keylogger, rootkit, RAT и т.н.) по наблюдавания модел на поведение.
REQ.289.	Решението трябва да може да използва YARA правила за разпознаване на зловреден код.
REQ.290.	Решението трябва да може да се свързва с файлови сървъри, използвайки протоколите Server Message Block или Internet File System, за анализ на съхранени файлове.

REQ.291.	Решението трябва да позволява конфигурирането на различни споделени файлови директории, в зависимост от операционната система, която ще се използва за извършването на анализ на зловреден код.
REQ.292.	Решението трябва да може автоматично да разпределя анализираните файлове към различни локации, изполвайки споделени мрежови дялове, според това дали имат зловредно поведение или нямат зловредно поведение.
REQ.293.	Решението трябва да може да изпраща автоматични известия чрез Syslog, HTTP, SNMP и SMTP протоколи.
REQ.294.	Решението трябва да позволява избирането на времевия интервал, през който да бъдат проверявани споделените дялове за нови файлове.
REQ.295.	Решението трябва да може да използва прокси с автентикация за достъпване на сървъра му за обновления.
REQ.296.	Решението трябва да работи с уеб-базирана конзола за управление, която да не изисква инсталирането на допълнителен софтуер за достъпването ѝ.
REQ.297.	Решението трябва да позволява конфигурирането на ACL списък, за да се ограничат позволените свързвания с интерфейса за управление.
REQ.298.	Решението трябва да използва криптиран канал за комуникация между администраторите и конзолата за управление. Също така, трябва да позволява вмъкването на собствени дигитални сертификати на организацията, използвани за криптиране на връзката.
REQ.299.	Решението трябва да позволява локално задаване на дата и час или чрез синхронизация с NTP сървър.
REQ.300.	Решението трябва да позволява създаването на акаунти с различни роли и права, например администратори и потребители, които само следят за аларми.
REQ.301.	Решението трябва да позволява автентикиране към конзолата за управление чрез RADIUS, TACACS + и LDAP.
REQ.302.	Решението трябва да може автоматично да изпраща известия и периодично създадени отчети за „здравето“ си, използвайки SMTP.
REQ.303.	Решението трябва да позволява извличането на аларми и отчети за активността на зловреден код под формата на PDF.
REQ.304.	Решението трябва да позволява конфигурирането на съобщение, което да се показва при вписване в конзолата за управление.
REQ.305.	Решението трябва да може да се интегрира със специализирано оборудване за централизирано управление, което да може да корелира резултатите от анализите и да разпространява индикаторите за компроментиране до другите подсистеми за анализ на зловреден код.
REQ.306.	Решението трябва да може да се интегрира с Endpoint Detection and Response системи, като да може да получава артефакти от зловреден код уловен от софтуерните агенти на такъв тип система, инсталирани на ниво крайна точка или сървър.
REQ.307.	Решението трябва да може лесно да се интегрира с други подсистеми за мрежова защита и за email защита, за да се предостави информация в реално време за зловредни мрежови заявки

	(callbacks) и за споделяне на локално генерираните индикатори за компроментиране от анализите.
Хардуерни изисквания – 1 брой	
REQ.308.	Устройството да е с максимална големина 1RU
REQ.309.	Устройството да разполага с поне 4TB за съхранение на данни
REQ.310.	Устройството да разполага минимално със следните портове за свързване с мрежата: 2x 10/100/1000BASE-T Ports
REQ.311.	Допълнителни портове: сериен порт, 4x Type A USB, IPMI, VGA
REQ.312.	Резервирано захранване – 1+1
REQ.313.	Устройството да може да извършва минимално 8200 анализа на ден.
REQ.314.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
Гаранция и поддръжка:	
REQ.315.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.316.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.317.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.318.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.

7. **Подсистема за динамичен анализ на зловреден код и защита от кибератаки за мрежови файлови дялове (лаборатория) за динамичен анализ на зловреден код**

Общи изисквания	
REQ.319.	Тип решение: 1 брой хардуер с вграден софтуер и 5-годишна поддръжка, 5-годишен абонамент за прилежащи услуги
REQ.320.	Решението трябва да може да анализира файлове, използвайки sandbox технология, която да може да засича непознат „zero-day" зловреден код, вграден във файловете.
REQ.321.	Решението трябва да може да получава автоматично данни за заплахи от засечени такива при други клиенти на вендора от цял свят.
REQ.322.	Решението трябва да може да извършва рекурсивни автоматични сканирания, сканирания по времеви график и сканирания по ръчна заявка от администратор, за всички достъпни мрежови файлови дялове, за да да може да идентифицира и сложи под карантина всички засечени вируси по съхранените файлове, без да има значително влияние върху производителността на системите.
REQ.323.	Решението да позволява задаването на различни настройки за всяко сканиране, като да могат да се задават различни файлови типове или конкретни файлове да могат да бъдат сложени в „бял списък", за да са изключени от сканирането.
REQ.324.	Решението трябва да позволява паузиране и продължаване на сканирания, които се извършват в даден момент (в реално време).
REQ.325.	Решението трябва да може да премества безопасните файлове в определени локации, а заразените файлове да може да премества в отделена карантина.

REQ.326.	Решението трябва да може да връща файлове в първоначалните им локации, след като са освободени от карантината.
REQ.327.	Решението трябва да може да издава пълни отчети за поведението на файловете – прилежащи процеси, достъп до файловете/записани файлове на дисковото пространство, промени в регистрите на операционната система.
REQ.328.	Решението трябва да може да споделя откритите от него индикатори за компроментиране с останалите подсистеми, за динамичен анализ на зловреден код и за разследвания за кибератаки, също така да може и да получава индикатори за компроментиране от тях.
REQ.329.	Решението трябва да предоставя настройки на филтри при сканирането на файлове, според типа на файловете, локацията им, последната дата на модифициране.
REQ.330.	Решението трябва да позволява използването на YARA правила, версия 3.4.
REQ.331.	Решението трябва да може да извършва освен динамичен анализ, така и статичен анализ. Администраторите трябва да могат да избират дали да се извършва статичния анализ.
REQ.332.	Решението трябва да може да анализира файлове с големина до поне 1024 MB. Максималният размер на файловете, които ще се анализират, да може да бъде променян.
REQ.333.	Решението трябва да може да прави морфологичен разбор на .eml файлове.
REQ.334.	Решението трябва да може да извлича прикачени файлове от .eml файлове. Броя на прикачени файлове, които да се анализират, трябва да може да бъде променян.
REQ.335.	Решението трябва да може да създава локални дефиниции (signatures) на засечените зловредни файлове след динамичен анализ. Администраторите трябва да могат да конфигурират времето на изтичане на валидността на локалните дефиниции.
REQ.336.	Решението трябва да може да се интегрира по подразбиране с Microsoft Office 365 за обработка на файлове.
REQ.337.	Решението трябва да може да се интегрира по подразбиране с Microsoft OneDrive за обработка на файлове. Решението трябва да може да извършва динамичен анализ на файловете в облачното пространство на OneDrive.
REQ.338.	Решението трябва да може да се интегрира по подразбиране с Microsoft SharePoint Online, за защитено споделяне на файлове.
REQ.339.	Решението трябва да може да изпраща известия за събития по email, HTTP, Rsyslog, SNMP в XML, JSON или в текстов формат.
REQ.340.	Решението трябва да поддържа следните протоколи: CIFS, NFS, WebDAV, Secure WebDAV.
REQ.341.	Решението трябва да позволява избирането на кои файлови хранилища да се сканират, директно от графичния интерфейс за управление.
REQ.342.	Решението трябва да може да извлича първоначална информация за споделените дискови пространства, като например брой и тип на файловете на тях, за да може по-лесно да се определят критериите за сканирането им от решението.
REQ.343.	Решението трябва да предоставя информация за резултатите след извършване на сканиране.
REQ.344.	Решението трябва да може да предоставя детайлни отчети във формати .xml, .json, .csf и текстов формат, както и обобщителни отчети в .pdf формат.

REQ.345.	Решението трябва да позволява определянето на времеви график за автоматично изготвяне и изпращане на отчети.
REQ.346.	Решението трябва да позволява лесно извличане на резултати от анализи в PDF формат.
REQ.347.	Решението трябва да поддържа ролево-базиран достъп до конзолата за управление.
REQ.348.	Решението трябва да може да се интегрира с подистемата за централизирано управление и да може да се конфигурира от нея. Трябва да могат да се получават системни обновления през подсистемата за централизирано управление и да се обменят аларми и известия.
REQ.349.	Решението трябва да може да анализира файловете в локален sandbox, както и да може да изпраща файловете за анализ към външен sandbox, когато устройството е претоварено.
REQ.350.	Решението трябва да разполага с IPMI интерфейс.
REQ.351.	Решението трябва да поддържа AAA протокол за контрол на потребителския достъп.
REQ.352.	Решението трябва да разполага с вградени функции за филтриране на IP адреси, за да се защити интерфейса за управление от нежелан достъп.
REQ.353.	Решението трябва да позволява определянето на използваните ресурси за sandbox анализ, за да се избегне претоварване на системата.
REQ.354.	Решението трябва да поддържа наблюдение на показатели чрез SNMP.
REQ.355.	Решението трябва да предоставя функции за защитено изтриване на съхранени данни.
REQ.356.	Решението трябва да може да използва поне 190 виртуални машини за sandbox анализ по едно и също време.
REQ.357.	Решението трябва да може да извършва автоматичен анализ на поне 60000 потенциално зловредни обекта на ден.
REQ.358.	Решението трябва да може да докладва за опитите за мрежово свързване на анализираните обекти във виртуалните машини.
REQ.359.	Решението да може да извършва следствен анализ на откритите зловредни файлове и да може да предоставя копие на бинарния им (двоичен) код, както и PCAP файл с опитите им за мрежови свързвания, заедно с всички посетени URL адреси.
REQ.360.	Решението трябва да може да извършва динамичен анализ за зловреден код, да може да се обновява и да може да му се предоставя нова информация за заплахи, дори в offline режим, без да има връзка с Интернет.
REQ.361.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението трябва да използва собствен, специално изграден хипервайзор.
REQ.362.	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques).
REQ.363.	Решението трябва да разполага с графичен интерфейс, където да се изобразяват пълните детайли от извършения анализ на зловреден код.
REQ.364.	Решението трябва да позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите трябва да могат да променят поне следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, използван Outlook акаунт, използвани език и часова зона.

REQ.365.	Решението трябва да може да тества и засича зловреден код в различни операционни системи на виртуалните машини за sandbox анализ, с различни версии на service pack, като да се поддържат както x64, така и x86 архитектури, под Windows и под Mac.
REQ.366.	Решението трябва да може да извършва детайлен анализ и да открива зловреден код в следните файлови формати (минимално): изпълними .exe файлове, JAVA, PDF, MS Office документи, често срещани мултимедийни файлови формати като JPEG, QuickTime, MP3, архиви тип ZIP/RAR/7ZIP/TNEF, 3gp, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm.
REQ.367.	Решението трябва да позволява на администраторите да посочат кои приложения във виртуалните машини за анализ да стартират кои файлови типове.
REQ.368.	Решението трябва да може да извършва цялостен анализ локално, без да е необходимо да излиза информация извън структурите на организацията.
REQ.369.	Решението трябва да поддържа LDAP или RADIUS методи за вписване на потребителите (минимално).
REQ.370.	Решението трябва да разполага с команден и с графичен интерфейс (достъпен през стандартен уеб-браузър) за централизирано управление.
REQ.371.	Решението трябва да може да работи в следните режими (за анализиране на файлове): • Сканиране по ръчни заявки (on-demand, с възможност и за анализ на отделни файлове) • Продължително сканиране на посочени файлови хранилища.
REQ.372.	Решението трябва да позволява избирането на различни локации за преместване на файлове след анализ според това дали са със статус на „добър“, „неизвестен“ или „лош“.
Хардуерни изисквания – 1 брой	
REQ.373.	Устройството да е с максимална големина 2RU
REQ.374.	Устройството да разполага с поне 2TB за съхранение на данни
REQ.375.	Устройството да разполага минимално със следните портове за свързване с мрежата: 4x 1GigE BaseT
REQ.376.	Допълнителни портове: сериен порт, 4x Type A USB, IPMI
REQ.377.	Резервирано захранване – 1+1
REQ.378.	Устройството да може да анализира минимално 60000 файла на ден.
REQ.379.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
Гаранция и поддръжка:	
REQ.380.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.381.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.382.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.383.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.

8. **Подсистема за улавяне на мрежови пакети, разследвания и централизиран анализ и визуализация**

Общи изисквания	
REQ.384.	Тип решение: • 1 брой хардуер за улавяне на мрежови пакети, с вграден софтуер и 5-годишна поддръжка; • 1 брой хардуер за разследвания и централизиран анализ и визуализация, с вграден софтуер и 5-годишна поддръжка;
REQ.385.	Решението трябва да има пълна видимост над мрежовия трафик, чрез високоскоростно улавяне на мрежови пакети и анализ при мрежова производителност от 1800 Mbps за 4 интерфейса на ниво gateway. Решението трябва да може да се поставя в TAP/SPAN режим на работа, като да може да получава мрежовите данни след SSL декриптиране от настоящо решение за SSL декриптиране на организацията от трети производител (да има възможност за интеграция).
REQ.386.	Решението да има възможност за изключително бързо (в реално време) записване и индексиране на мрежови трафик.
REQ.387.	Решението трябва да може да улавя, търси и анализира информацията от мрежовите пакети и сесии.
REQ.388.	Решението трябва да може да чете и записва пакети в PCAP формат.
REQ.389.	Решението трябва да позволява извършването на филтрирани търсения, използвайки често срещани стойности за адрес, приложение, протокол, VLAN, MPLS, метаданни от мрежовата връзка.
REQ.390.	Решението трябва да поддържа интеграция с подсистема за засичане, защита и разследнване на непознати заплахи на ниво крайна точка, за да може да получава информация за вътрешно наблюдаваните IP адреси от крайните точки и за да може да извлича потребителските имена, асоциирани с дадено име на хост.
REQ.391.	Решението трябва да може да анализира мрежови сесии и да извлича файлове от тях.
REQ.392.	Решението трябва да позволява на анализаторите да търсят в мрежовия трафик ключови думи и регулярни изрази на ниво приложен слой.
REQ.393.	Решението трябва да поддържа сложни заявки, използващи булева логика.
REQ.394.	Решението трябва да може да се интегрира и изпраща извлечени файлове от мрежови сесии директно към подсистема (лаборатория) за динамичен анализ на зловреден код.
REQ.395.	Решението трябва да може да реконструира уеб-страници и email съобщения от уловения мрежови трафик. Също така, трябва да може да реконструира POP3/IMAP/FTP/SMB.
REQ.396.	Решението трябва да може да извлича данни от много големи файлове с мрежови трафик, до 1 гигабайт.
REQ.397.	Решението трябва да може да кодира/декодира следните формати от данни: Base64, gzip, HEX, HEXDUMP, JSON, URL, XOR.
REQ.398.	Решението трябва да позволява определянето на собствени правила, на базата на които да се улавя и съхранява мрежовия трафик за по-нататъшен анализ.

REQ.399.	Решението трябва да може да анализира в детайли следните протоколи: DCE-RPC, IPv6, SMB, DHCP, IRC, SMB2, DNS, MODBUS, SMTP, ERSPAN, MPLS, SSL, FTP, MSN, SSH, GRE, POP3, TCP, HTTP, PPP, TEREDO, ICMPv4, RDP, TLS, ICMPv6, RTSP, UDP, IMAP, SCTP, VLAN, IPv4, SIP, IPFIX, NETFLOWv5, NETFLOWv9.
REQ.400.	Решението трябва да позволява търсене в индексираните метаданни на следните протоколи: HTTP, DNS, SMTP, POP3, IMAP, SSL, TLS, FTP, SSH и MODBUS.
REQ.401.	Решението трябва да може да разпознава минимално следните приложения: AFP, Aimini, Amazon, Apple, AppleiCloud, AppleiTunes, AppleJuice, Armagetron, AVI, Ayiya, BattleField, BGP, BitTorrent, CiscoSkinny, CiscoVPN, Citrix, Citrix_Online, CNN, Collectd, Corba, Crossfire, DCE_RPC, DHCP, DHCPV6, DirectConnect, Direct_Download_Link, DNS, Dofus, DropBox, eBay, eDonkey, EGP, EPP, Facebook, FacebookChat, FastTrack, Fiesta, Filetopia, Flash, Florensia, FTP, FTP_CONTROL, FTP_DATA, GMail, Gnutella, Google, GoogleMaps, GRE, GrooveShark, GTP, Guildwars, H323, HalfLife2, HTTP, HTTP_Application_ActiveSync, HTTP_APPLICATION_VEOHTV, HTTP_Connect, HTTP_Proxy, IAX, IceCast, ICMP, ICMPV6, IGMP, IMAP, IMAPS, iMESH, IPP, IPsec, IP_in_IP, IRC, Jabber, Kerberos, Kontiki, LastFM, LDAP, LLMNR, LotusNotes, MapleStory, MDNS, Meebo, Megaco, MGCP, MMS, Move, MPEG, MSN, MsSQL, MySQL, NetBIOS, NetFlix, NFS, NOE, NTP, OggVorbis, OpenFT, OpenVPN, Oracle, Oscar, OSPF, Pandora, Pando_Media_Booster, PcAnywhere, POP, POP3, POPS, PostgreSQL, PPLive, PPStream, PPTP, QQ, QQLive, Quake, QuickTime, Radius, RDP, RealMedia, Redis, RemoteScan, RSYNC, RTCP, RTMP, RTP, RTSP, SAP, SCTP, sFlow, ShoutCast, SIP, SkyFile_PostPaid, SkyFile_PrePaid, SkyFile_Rudics, Skype, SMB, SMTP, SMTPS, SNMP, SOCKS4, SOCKS5, Socrates, Sopcast, Soulseek, Spotify, SSDP, SSH, SSL, SSL_No_Cert, Stealthnet, Steam, STUN, Syslog, TDS, TeamSpeak, TeamViewer, Telegram, Telnet, TFTP, Thunder, TOR, TruPhone, Tuenti, Tvants, TVUplayer, Twitter, UbuntuONE, Unencryped_Jabber, Unknown, UPnP, Usenet, VEOHTV, VHUA, Viber, VMware, VNC, VRRP, Warcraft3, Webex, WebM, Whois-DAS, WhatsApp, Wikipedia, WindowsMedia, WindowsUpdate, WinMX, WorldOfKungFu,WorldOfWarcraft, Xbox, XDMCP, Yahoo, YouTube, Zattoo, ZeroMQ.
REQ.402.	Решението трябва да може да анализира следните видове мрежови трафик: използващ IPv4 протокол; използващ IPv6 протокол.
REQ.403.	Решението трябва да предоставя на администраторите разбираем и с възможност за модифициране интерфейс със списъци, графики и географски карти.
REQ.404.	Решението трябва да позволява на администраторите лесно и бързо да извършват „reverse DNS lookup“ и „whois“ проверки директно от уеб интерфейса.
REQ.405.	Решението трябва да позволява на анализаторите да преглеждат данните на ниво мрежова връзка, пакет и payload.
REQ.406.	Решението трябва да може да приема аларми от другите подсистеми за киберсигурност.
REQ.407.	Решението за улавяне на мрежови пакети трябва да използва „full disk encryption“ метод за криптиране на събраните данни и метаданни.
REQ.408.	Решението за улавяне на мрежови пакети трябва да може да се интегрира с SAS RAID или с HBA контролер, за да се гарантира непрекъснат процес на събирането на мрежови пакети.
REQ.409.	Решението трябва да разполага с IPMI интерфейс.

REQ.410.	Решението трябва да поддържа автентикация на потребителите с протоколи PAM/LDAP/RADIUS/TACACS+. Да се поддържа ролево-базирано управление, потребителите да могат да имат различни роли (администратор, анализатор, т.н.)
REQ.411.	Решението трябва да може да засича извличане на данни извън организацията.
REQ.412.	Решението трябва да поддържа Suricata правила за дефиниции/алармиране.
REQ.413.	Решението трябва да позволява задаването на правила за филтриране на мрежовия трафик. Правилата са необходими за намаляване на обема анализиран трафик. Тези правила трябва да са наложени директно на хардуерните интерфейси за улавяне на трафика, преди да затормозят централният процесор на системата. Да може да се филтрира минимално на база следните параметри: src IP, src port, dst IP, dst port.
REQ.414.	Решението трябва да може да извлича метаданни от уловения мрежови трафик през HTTP.
REQ.415.	Решението трябва да може да индексира в реално време уловените мрежови пакети, използвайки маркери за време и атрибутите на мрежовите свързвания. Да могат да се извличат индекса на потока от данни и метаданните на мрежовата връзка в JSON формат.
REQ.416.	Решението трябва да предоставя информация за собствените си процеси и за складираните данни, за да може да се планира капацитета в бъдеще.
REQ.417.	Решението трябва да позволява да му се наблюдават параметрите по производителността чрез SNMP.
REQ.418.	Решението трябва да предоставя възможност за сигурно изтриване на данните от дисковото му пространство, чрез презаписване (overwrite) на данните множество пъти.
REQ.419.	Решението трябва да може да се интегрира с източници на информация за заплахи.
REQ.420.	Решението трябва да позволява добавянето на множество нови индикатори за компроментиране чрез формати STIX и OpenIOC.
REQ.421.	Решението трябва да позволява определяне на времеви интервал за автоматично търсене за индикатори за компроментиране в събраните метаданни и да може да вдига аларми за тях.
REQ.422.	Решението трябва да поддържа изпозлването на reverse SSH и HTTPS тунели, за да може да се интегрира със системи от външна мрежа.
REQ.423.	Решението трябва да поддържа автентикация с използване на smart карти.
REQ.424.	Решението трябва да предоставя достъп за търсене в съхранените метаданни.
REQ.425.	Решението трябва да може да се интегрира и да приема метаданни на слой 7 от подсистема за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво, както и да може да изисква уловени пакети по конкретно събитие, за което е вдигната аларма.
REQ.426.	Решението трябва да разполага с API интерфейс.
REQ.427.	Решението за улавяне на мрежови пакети трябва да е изградено с подсилена откъм сигурност, заключена операционна система.
REQ.428.	Решението за улавяне на мрежови пакети трябва да може да съхранява събраните PCAP данни и метаданни за поне 14 дена, при събиране на данни 8 часа на ден при количество трафик от 1 Gbps.
Хардуерни изисквания за хардуерно устройство за улавяне на мрежови пакети	
REQ.429.	Устройството да е с максимална големина 2U

REQ.430.	Устройството да разполага с поне 95TB за съхранение на данни, с възможност за разширяване на обема със скачено SAS дисково пространство
REQ.431.	Устройството да разполага минимално със следните портове за свързване с мрежата: 4 x 10GE SFP+
REQ.432.	Допълнителни портове: 2 x 1GbE портове за управление
REQ.433.	Резервирано захранване – 1+1
REQ.434.	Устройството да може да записва мрежови данни със скорост от 1800 Mbps
Хардуерни изисквания за хардуерно устройство за разследвания и централизиран анализ и визуализация	
REQ.435.	Устройството да е с максимална големина 2U
REQ.436.	Устройството да разполага с поне 45TB за съхранение на данни
REQ.437.	Резервирано захранване – 1+1
Гаранция и поддръжка:	
REQ.438.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.439.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.440.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.441.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.

ПРИЛОЖЕНИЕ № 2.6

ДО
„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД
ГР. СОФИЯ, УЛИЦА „ПАНАЙОТ ВОЛОВ“ № 2

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

Наименование на обществената поръчка:	***„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите"***
Наименование на обособена позиция, за която участникът подава оферта	***Обособена позиция № 6: „Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити кибер заплахи“***
Наименование на участника:	***КОМПЮТЪР 2000 България***
Правно-организационна форма на участника:	***ЕООД***
Седалище по регистрация и адрес на управление:	**Гр. София, бул. „Шипченски проход“ № 63, Производствена сграда Електроника, ет. 4**
ЕИК / Код по регистър БУЛСТАТ/ регистрационен номер или друг идентификационен код:	**831816173**
Представляващ	***Анелия Илиева Костадинова – Управител***

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,

След запознаване с документацията за участие в обществената поръчка с горепосочения предмет, ние предоставяме следното техническо предложение по горецитираната обособена позиция, съдържащо:

Заличаването на информация в документа е на основание чл. 4 от Общ регламент за защита на данните.

I.ПРЕДЛОЖЕНИЕ ЗА ИЗПЪЛЕНИЕ НА ПОРЪЧКАТА

В качеството си на представляващ участника, декларирам, че сме запознати с условията на поръчката и с подаването на настоящото предложение удостоверявам следното:

1. **Предмет на обществената поръчка:**

1.1. Декларирам, че представляваният от мен участник ще изпълни поръчката, съобразявайки се с условията по изпълнение, посочени от възложителя в документацията за обществената поръчка.

1.2. Запознати сме, че съгласно чл. 39, ал. 1 от Правилника за прилагане на Закона за обществените поръчки (ППЗОП) с подаването на офертата по настоящата обществена поръчка се счита, че се съгласяваме с всички условия на възложителя, в т.ч. с определения срок за валидност на офертата и с проекта на договор, неразделна част от документацията за обществената поръчка.

1.3. Задължаваме се да извършим следните дейности:

1.3.1. доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричано по-нататък за краткост „оборудването"), подробно описано по вид, количество и технически характеристики в Техническата спецификация, Приложение 1.6. към нея, относимо към настоящата обособена позиция, за която подаваме оферта и настоящето Техническо предложение.

1.3.2. гаранционно обслужване на доставеното по т. 1.3.1. оборудване (наричано по-нататък алтернативно „гаранция и поддръжка"), осигурено в рамките на срока по т. 5.2. в съответствие с предписанията на производителя, изискванията на договора за обществена поръчка и приложенията към него.

1.4. Подробно описание на вида, количеството и техническите характеристики на доставеното от нас оборудване, хардуер и софтуер, е описано, както следва:

1.4.1. Подсистема за засичане, разследвания и защита от познати и непознати заплахи на ниво крайна точка

Изискано от Възложителя		Предложено от участника
А.		**Б.**
Общи изисквания		
REQ.1.	Брой на крайните точки: 8000	Предлаганата подсистема за засичане, разследвания и защита от познати и непознати заплахи на ниво крайна точка е предназначена за **8000 крайни точки**
REQ.2.	Тип решение: 1 брой основен хардуер с вграден софтуер и 5-годишна поддръжка, 1 брой хардуер за DMZ с вграден софтуер и 5-годишна поддръжка, включени 8000 лицензи (софтуерни агенти) за поставяне на крайните точки, също с 5-годишна поддръжка, 5-годишен абонамент за прилежащи услуги към 8000-те агента	Предлаганата подсистема за засичане, разследвания и защита от познати и непознати заплахи на ниво крайна точка включва: **1 брой основно хардуерно устройство FireEye HW-4502 HX с включена 5-годишна поддръжка; 1 брой хардуерно устройство за DMZ с вграден софтуер с включена 5-годишна поддръжка – FireEye HW-4502D HX DMZ; 8000 лицензи** (софтуерни агенти) за поставяне на крайните точки **FireEye Endpoint Security Power-9999 с включена 5-годишна софтуерна поддръжка; 5-годишен абонамент за прилежащи услуги към 8000-те агента FireEye DTI Endpoint Security Power Off Sub-9999-5Y с включена 5-годишна софтуерна поддръжка;**
REQ.3.	Решението трябва да е споменато в документа на Gartner: Market Guide for Endpoint Detection and Response Solutions.	Решението се споменава в документа на Gartner: Market Guide for Endpoint Detection and Response Solutions.
REQ.4.	Решението трябва да притежава следните сертификати: Federal Information Processing Standards (FIPS) 140-2 и Common Criteria (CC).	Решението притежава следните сертификати: Federal Information Processing Standards (FIPS) 140-2 и Common Criteria (CC).

<table>
<tr><td></td><td></td><td>https://www.niap-ccevs.org/MMO/Product/st_vid10892-agd.pdf</td></tr>
<tr><td>REQ.5.</td><td>Решението да предоставя цялостна защита за крайни точки, включително засичане и превенция на атаки, да предоставя функции за разследване и почистване (в зависимост от метода на имплементация на решението), като да се поддържат минимално следните операционни системи на крайните точки: Window (XP, 7, 8, 10, Server 2003, 2008, 2012, 2016), mac OS X и Linux (RHEL, CentOS, Ubuntu, Suse).</td><td>Решението предоставя цялостна защита за крайни точки, включително засичане и превенция на атаки, предоставя функции за разследване и почистване (в зависимост от метода на имплементация на решението), като се поддържат следните операционни системи на крайните точки: Window (XP, 7, 8, 10, Server 2003, 2008, 2012, 2016), mac OS X и Linux (RHEL, CentOS, Ubuntu, Suse).

https://docs.fireeye.com/docs/docs_en/Agent/sw/32/SSS/Agent_SSS_32_en.pdf

Table 5. Requirements for Windows operating systems.
<table>
<tr><th>WINDOWS OPERATING SYSTEM VERSIONS</th><th>MINIMUM SYSTEM MEMORY (RAM)</th></tr>
<tr><td>XP SP3 (32-bit)
Server 2003 R2 SP2 (32-bit, 64-bit)</td><td>512 MB</td></tr>
<tr><td>Server 2016 (64-bit)</td><td>2 GB</td></tr>
<tr><td>Vista SP1 and higher (32-bit, 64-bit)
Windows 7and Win 7 SP1 (32-bit, 64-bit)
Win 8 (32-bit, 64-bit)
Win 8.1 (32-bit, 64-bit)
Win 10 (32-bit, 64-bit)</td><td>1 GB (32-bit),
2 GB (64-bit)</td></tr>
<tr><td>Server 2008 (32-bit, 64-bit)
Server 2008 R1, R2, R2 SP1, R2 SP2 (32-bit, 64-bit)
Server 2012 (32-bit, 64-bit)
Server 2012 R2 (64-bit)
Server 2016 (64-bit)
Server 2019 (64-bit)</td><td>2 GB (64-bit)</td></tr>
</table>
Table 6. Requirements for macOS.
<table>
<tr><th>MAC OS VERSIONS</th><th>MINIMUM SYSTEM MEMORY (RAM)</th></tr>
<tr><td>Mavericks 10.9 (64-bit)
Yosemite 10.10 (64-bit)
El Capitan 10.11 (64-bit)
Sierra 10.12 (64-bit)
High Sierra 10.13 (64-bit)
Mojave 10.14 (64-bit)
Catalina 10.15 (64-bit)</td><td>1 GB</td></tr>
</table>
Table 7. Requirements for Linux operating systems.
<table>
<tr><th>LINUX OPERATING SYSTEM VERSION</th><th>MINIMUM SYSTEM MEMORY (RAM)</th></tr>
<tr><td>RHEL 6.8+ (64-bit)
RHEL 7.1+ (64-bit)
RHEL 8 (64-bit)
CentOS 6.9+ (64-bit)
CentOS 7.1+ (64-bit)
CentOS 8 (64-bit)
SUSE 11.3, 11.4,12.2,12.3,15
Open SUSE 15.1
Ubuntu 12.04, 14.04, 16.04, 18.04, 19.04, 20.04
Amazon Linux AMI 2018.3, AM2
Oracle Linux 6.10, 7.6</td><td>2 GB</td></tr>
</table></td></tr>
<tr><td>REQ.6.</td><td>Решението трябва да включва специализирано устройство (хардуер), което да служи за</td><td>Решението включва специализирано устройство (хардуер), което служи за централизирано</td></tr>
</table>

	централизирано управление на инсталираните агенти по крайните точки, за да могат да се наблюдават всички защитени крайни точки за съмнително зловредно поведение и да може да се извършва централизирано разследване.	управление на инсталираните агенти по крайните точки, като по този начин могат да се наблюдават всички защитени крайни точки за съмнително зловредно поведение и може да се извършва централизирано разследване. Източник: ENDPOINT SECURITY SERVER SYSTEM ADMINISTRATION GUIDE RELEASE 5.0 Страница 17
REQ.7.	Агентите на решението трябва да могат да засичат, анализират и позволяват ответна реакция на напреднали кибератаки, използващи непознати „zero-day" уязвимости, независимо дали крайните точки се намират във или извън мрежата на организацията.	Агентите на решението могат да засичат, анализират и позволяват ответна реакция на напреднали кибератаки, използващи непознати „zero-day" уязвимости, независимо дали крайните точки се намират във или извън мрежата на организацията. Източник: ENDPOINT SECURITY SERVER SYSTEM ADMINISTRATION GUIDE RELEASE 5.0 Страница 18
REQ.8.	Комуникацията между софтуерните агенти и централизираното управление трябва да е криптирана.	Комуникацията между софтуерните агенти и централизираното управление е криптирана. Източник: PORTS AND PROTOCOLS REFERENCE GUIDE Източник: Endpoint Security Threat Protection System — Agent Страници 8-9

<table>
<tr><td></td><td></td><td>

Endpoint Security Threat Protection System — Agent

Source Device	Destination Device	Destination Port	User Configurable	Notes
Agent – For HX and MIR 3.x and later				
Agent	DMZ Server Primary MIR Controller HX Server	TCP HTTP 80	No	Fast Poll
Agent	DMZ Server Primary MIR Controller HX Server	TCP HTTPS 443	No	Regular Poll Audits and Data Collection for MIR

Source Device	Destination Device	Destination Port	User Configurable	Notes
Agent	Primary MIR Controller HX Server DMZ Server	TCP HTTPS 443	No	Agent Provisioning Containment Requests, Triage and File Acquisitions for HX

</td></tr>
<tr><td>REQ.9.</td><td>Агентите на крайните точки трябва да са с малък размер, с минимално влияние на производителността на системите, като да се предоставя механизъм за контролиране на какъв процент от процесорната мощ на крайните точки да се използва за анализ и превенция на атаки, така че да не се влияе на нормалната работа на потребителите.</td><td>

Агентите на крайните точки са с малък размер, с минимално влияние на производителността на системите, като се предоставя механизъм за контролиране на какъв процент от процесорната мощ на крайните точки се използва за анализ и превенция на атаки, така че да не се влияе на нормалната работа на потребителите.

Източник: AGENT ADMINISTRATION GUIDE RELEASE 32.30.0

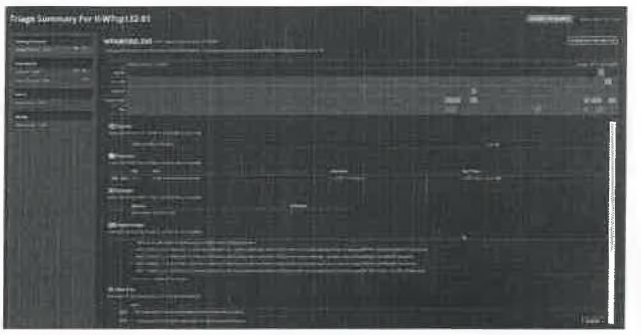
Страници: 331, 333-334

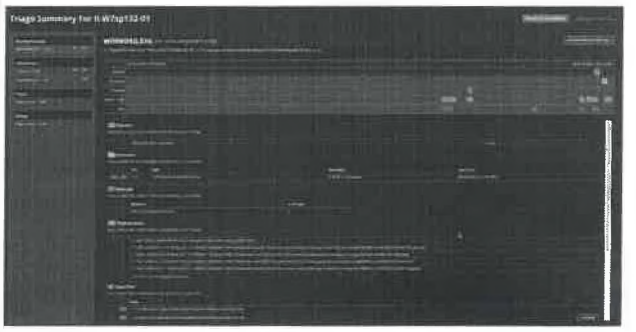
Process	Description	Mem (MB)
Service	Main Parent Process	15
ProRem	Protection & Remediation Service	7
Eventor	Real-time Indicator Detection	92
AV	Malware (Signature and Heuristic Detection)	218
MG	MalwareGuard	309
ExG	Exploit Guard Protection	18

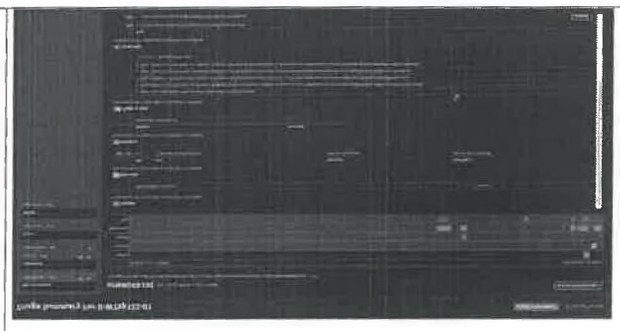
Table 2 – xAgent Engine Memory Requirements

</td></tr>
<tr><td>REQ.10.</td><td>Решението трябва да предоставя минимално следните функционалности:
• Корелация в реално време на индикаторите за компроментиране на ниво крайна точка.</td><td>Решението предоставя следните функционалности:
• Корелация в реално време на индикаторите за компроментиране на ниво крайна точка.</td></tr>
</table>

	• Засичане и блокиране на exploit атаки, използвайки алгоритми за анализиране на поведението на приложенията. Засичане на ROP (Return Oriented Programming) атаки, reverse shell, heap spray, SEHOP corruption, атаки използващи Java уязвимости. • Засичане на зловредни файлове в реално време. • Сканиране на файлове използвайки антивирусни алгоритми с дефиниции и чрез евристичен анализ. • Сканиране на изпълними файлове чрез алгоритми за машинно обучение (machine learning). • Възможност за сортиране на информация, за да може да се потвърди наличието на дадена атака и за да може да се възпроизведе целия ѝ жизнен цикъл за анализ. • Автоматично създаване на графика с хронологично подредени събития, довели до компроментирането на дадена крайна точка. • Възможност за изключително бързо търсене в избрани крайни точки за зададени ключови думи, MD5 / SHA1 и SHA256 суми, сложни изрази, създадени файлове в зададен интервал от време, конкретни „бисквитки", име на DNS хост, конкретни драйвери, файлови атрибути, HTTP хедъри, IP адреси, използвани портове за мрежова комуникация и активни процеси, конкретни ключове в регистрите на операционната система, Windows събития. • Функцията за търсене на информация трябва да може да се използва директно от	• Засичане и блокиране на exploit атаки, използвайки алгоритми за анализиране на поведението на приложенията. Засичане на ROP (Return Oriented Programming) атаки, reverse shell, heap spray, SEHOP corruption, атаки използващи Java уязвимости. • Засичане на зловредни файлове в реално време. • Сканиране на файлове, използвайки антивирусни алгоритми с дефиниции и чрез евристичен анализ. • Сканиране на изпълними файлове чрез алгоритми за машинно обучение (machine learning). • Възможност за сортиране на информация, за да може да се потвърди наличието на дадена атака и за да може да се възпроизведе целия ѝ жизнен цикъл за анализ. • Автоматично създаване на графика с хронологично подредени събития, довели до компроментирането на дадена крайна точка. • Възможност за изключително бързо търсене в избрани крайни точки за зададени ключови думи, MD5 / SHA1 и SHA256 суми, сложни изрази, създадени файлове в зададен интервал от време, конкретни „бисквитки", име на DNS хост, конкретни драйвери, файлови атрибути, HTTP хедъри, IP адреси, използвани портове за мрежова комуникация и активни процеси, конкретни ключове в регистрите на операционната система, Windows събития. • Функцията за търсене на информация може да се използва директно от графичния интерфейс на решението, както и използвайки API интерфейс

	графичния интерфейс на решението, както и използвайки API интерфейс, така че да могат да се използват автоматизирани скриптове. • Да могат да се изолират заразените крайни точки директно от централизираното управление на решението (по заявка от администратор), позволявайки им комуникация само с посочени IP адреси (Endpoint containment).	така че могат да се използват автоматизирани скриптове. • Могат да се изолират заразените крайни точки директно от централизираното управление на решението (по заявка от администратор), позволявайки им комуникация само с посочени IP адреси (Endpoint containment). Източник: ENDPOINT SECURITY SERVER USER GUIDE RELEASE 5.0 Страници: 21-24, 27, 231, 240-242, 253-258, 308, 310-325 Източник: ENDPOINT SECURITY REST API GUIDE Страница 139 
REQ.11.	Решението трябва да може автоматично да събира и да предоставя информация за използвани уязвимости, процеси, домейни, регистри, файлове и мрежова активност за вдигнатите аларми. Информацията трябва да е	Решението може автоматично да събира и предоставя информация за използвани уязвимости, процеси, домейни, регистри, файлове и мрежова активност за вдигнатите аларми. Информацията е достъпна за преглед директно от

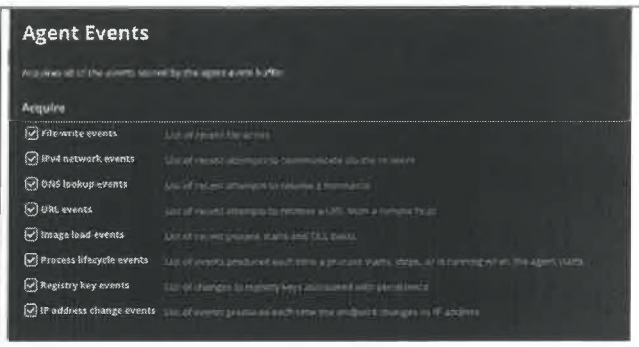
	достъпна за преглед директно от графичния интерфейс на конзолата за централизирано управление.	графичния интерфейс на конзолата за централизирано управление. **Източник: ENDPOINT SECURITY SERVER USER GUIDE RELEASE 5.0** Страници: 103, 308 
REQ.12.	Решението трябва да позволява извличането на файлове от системите, на които има инсталиран агент. За Windows операционни системи, решението трябва да може да извлича заключени или изтрити файлове, ако те все още не са презаписани от нова информация.	Решението позволява извличането на файлове от системите, на които има инсталиран агент. За Windows операционни системи, решението може да извлича заключени или изтрити файлове, ако те все още не са презаписани от нова информация. Източник: ENDPOINT SECURITY SERVER USER GUIDE RELEASE 5.0 Страници: 27, 291-294
REQ.13.	Решението трябва да позволява извличането на файлове, които са записани на крайните точки в следствие на зловредна активност, директно от интерфейса за разследване на аларми на централизираното управление.	Решението позволява извличането на файлове, които са записани на крайните точки в следствие на зловредна активност, директно от интерфейса за разследване на аларми на централизираното управление. **Източник: ENDPOINT SECURITY SERVER USER GUIDE RELEASE 5.0** Страници: 308, 310-325

		
REQ.14.	Функцията за извличане на файлове трябва да може да се използва директно от графичния интерфейс на решението, както и използвайки API интерфейс, така че да могат да се използват автоматизирани скриптове.	Функцията за извличане на файлове може да се използва директно от графичния интерфейс на решението, както и използвайки API интерфейс, така че да могат да се използват автоматизирани скриптове. Източник: ENDPOINT SECURITY SERVER USER GUIDE RELEASE 5.0 Страници: 27, 291-294 Източник: ENDPOINT SECURITY REST API GUIDE Страници: 806-810
REQ.15.	Решението трябва да може автоматично да генерира пакети с данни от крайните точки (endpoint triage), за да се подпомогне разследването на аларми. Пакетите с данни трябва да съдържат информация за системните параметри на крайната точка, процесите, файловете, регистрите, потребителските акаунти, история на браузването.	Решението може автоматично да генерира пакети с данни от крайните точки (endpoint triage), за да се подпомогне разследването на аларми. Пакетите с данни съдържат информация за системните параметри на крайната точка, процесите, файловете, регистрите, потребителските акаунти, история на браузването.

		Източник: ENDPOINT SECURITY SERVER USER GUIDE RELEASE 5.0 Страници: 288-289
REQ.16.	Решението трябва да позволява извличането на информация за подпомагане на разследванията, като историята на извиканите shell команди, цялото дисково пространство на дадена крайна точка, цялата информация от паметта на крайната точка, историята на извиканите powershell команди, списък на процесите в паметта, списък на файловете на дисковото пространство на крайната точка.	Решението позволява извличането на информация за подпомагане на разследванията, като историята на извиканите shell команди, цялото дисково пространство на дадена крайна точка, цялата информация от паметта на крайната точка, историята на извиканите powershell команди, списък на процесите в паметта, списък на файловете на дисковото пространство на крайната точка. Източник: ENDPOINT SECURITY SERVER USER GUIDE RELEASE 5.0 Страница 397
REQ.17.	Решението трябва да може да получава индикатори за компроментиране директно от производителя и от другите подсистеми за киберсигурност, както и да се позволява създаването на собствени индикатори за	Решението може да получава индикатори за компроментиране директно от производителя и от другите подсистеми за киберсигурност, както и се позволява създаването на собствени индикатори за компроментиране от администраторите, също

	компроментиране от администраторите, също така да е възможна и интеграцията с външни източници на индикатори.	така да е възможна и интеграцията с външни източници на индикатори. Източник: ENDPOINT SECURITY SERVER USER GUIDE RELEASE 5.0 Страница 207
REQ.18.	Решението трябва да позволява наблюдението на крайни точки и засичане на вируси тип троянски кон, червеи, шпионски софтуер, adware, key logger вируси, rootkit вируси и exploit вируси, които се появяват след употребата на приложения като например Adobe Reader, Adobe Flash, Internet Explorer, Firefox, Google Chrome, Java, Microsoft Outlook, Microsoft Word, Microsoft Excel и Microsoft PowerPoint, включително да могат да се блокират и спират от агента заразените приложения.	Решението позволява наблюдението на крайни точки и засичане на вируси тип троянски кон, червеи, шпионски софтуер, adware, key logger вируси, rootkit вируси и exploit вируси, които се появяват след употребата на приложения като например Adobe Reader, Adobe Flash, Internet Explorer, Firefox, Google Chrome, Java, Microsoft Outlook, Microsoft Word, Microsoft Excel и Microsoft PowerPoint, включително могат да се блокират и спират от агента заразените приложения. Източник: ENDPOINT SECURITY SERVER USER GUIDE RELEASE 5.0 Страница 19
REQ.19.	Решението трябва да може да изпраща файлове за по-нататъшен анализ към подсистема за sandbox анализ, разположена локално в структурите на организацията (on premise).	Решението може да изпраща файлове за по-нататъшен анализ към подсистема за sandbox анализ, разположена локално в структурите на организацията (on premise). Източник: ENDPOINT SECURITY ENDPOINT ENRICHER MODULE USER GUIDE Страница 5
REQ.20.	Решението трябва да може да следи изпълнението на файлове, като да може да определи дали са изпълнени за първи път или пътя на изпълнение на файловете е променен. Тази информация (мета данни) трябва да може	Решението може да следи изпълнението на файлове, като и може да определи, дали са изпълнени за първи път или пътят на изпълнение на файловете е променен. Тази информация (мета

	да се изпраща към решение тип SIEM чрез интеграция.	данни) може да се изпраща към решение тип SIEM чрез интеграция. Източник: ENDPOINT SECURITY Process Tracker MODULE USER GUIDE v1.2.4 Страница 5
REQ.21.	Решението трябва да може да засича непознати „zero-day" атаки, като динамичния анализ на поведението на процесите трябва да работи минимално за .dll, .ocx, .sys и изпълними (.exe) файлове, като анализа да се извършва локално, без да е необходимо изпращането на проби към облачни услуги или трети OEM решения.	Решението може да засича непознати „zero-day" атаки, като динамичният анализ на поведението на процесите работи минимално за .dll, .ocx, .sys и изпълними (.exe) файлове, като анализът се извършва локално, без да е необходимо изпращането на проби към облачни услуги или трети OEM решения. Източник: ENDPOINT SECURITY SERVER USER GUIDE RELEASE 5.0 Страници: 19-20
REQ.22.	Агентите на решението трябва да могат да записват локално събитията свързани с работата с файлове (създаване, отваряне, модифициране), с мрежовите комуникации от крайните точки, DNS заявките, достъпените URL адреси, стартираните процеси, с използваните ключове от регистрите на операционната система.	Агентите на решението могат да записват локално събитията, свързани с работата с файлове (създаване, отваряне, модифициране), с мрежовите комуникации от крайните точки, DNS заявките, достъпените URL адреси, стартираните процеси, с използваните ключове от регистрите на операционната система. Източник: ENDPOINT SECURITY SERVER USER GUIDE RELEASE 5.0 Страници: 128-129

		
REQ.23.	Решението трябва да позволява да се изолират заразените крайни точки директно от централизираното управление на решението (по заявка от администратор), позволявайки им комуникация само с посочени IP адреси (Endpoint containment), така че да се спре разпространението на заразата по мрежата. Механизма трябва да позволява използването на различни роли на потребителите, които да правят заявки за изолиране на заразена крайна точка и които да одобряват заявките.	Решението позволява да се изолират заразените крайни точки директно от централизираното управление на решението (по заявка от администратор), позволявайки им комуникация само с посочени IP адреси (Endpoint containment), така че да се спре разпространението на заразата по мрежата. Механизмът позволява използването на различни роли на потребителите, които правят заявки за изолиране на заразена крайна точка и които одобряват заявките. Източник: ENDPOINT SECURITY SERVER USER GUIDE RELEASE 5.0 Страница 27 Capability / Description / Authorized AAA Roles Approve Containment / Approve containment requests and stop containment of host endpoints / admin, api_admin, ic_services, investigator
REQ.24.	Решението трябва да може централизирано да обновява софтуерната версия на инсталираните агенти.	Решението може централизирано да обновява софтуерната версия на инсталираните агенти. Източник: ENDPOINT SECURITY SERVER USER GUIDE RELEASE 5.0 Страница 78
REQ.25.	Решението трябва да разполага с механизми за собствена защита от спиране или рестартиране	Решението разполага с механизми за собствена защита от спиране или рестартиране на

	на инсталираните агенти, както и от инжектиране на нежелани процеси в тях.	инсталираните агенти, както и от инжектиране на нежелани процеси в тях. Източник: ENDPOINT SECURITY AGENT ADMINISTRATION GUIDE RELEASE 32.30.0 Страница 358
REQ.26.	Решението трябва да предоставя механизъм с използване на парола, за да се предотврати премахването на инсталиран агент от неоторизирано лице.	Решението предоставя механизъм с използване на парола, за да се предотврати премахването на инсталиран агент от неоторизирано лице. Източник: ENDPOINT SECURITY AGENT ADMINISTRATION GUIDE RELEASE 32.30.0 Страница 323
REQ.27.	Решението трябва да разполага с добре описан API интерфейс за интегриране.	Решението разполага с добре описан API интерфейс за интегриране. Източник: ENDPOINT SECURITY REST API GUIDE RELEASE 4.9
REQ.28.	Решението трябва да позволява администрация чрез уеб-базирана конзола, без да се изисква инсталирането на допълнителен софтуер за достъпването ѝ.	Решението позволява администрация чрез уеб-базирана конзола, без да се изисква инсталирането на допълнителен софтуер за достъпването ѝ. Източник: ENDPOINT SECURITY SERVER USER GUIDE RELEASE 5.0 Страница 31
REQ.29.	Решението трябва да позволява използването на прокси с оторизация за свързване със сървър за обновления на софтуера и информацията за нови заплахи.	Решението позволява използването на прокси с оторизация за свързване със сървър за обновления на софтуера и информацията за нови заплахи. Източник: ENDPOINT SECURITY SERVER SYSTEM ADMINISTRATION GUIDE RELEASE 5.0

		Страница 75
REQ.30.	Решението трябва да може да създава, съхранява и предоставя log файлове към трети решения, използвайки Syslog протокол, например за предоставяне на информация на решения от тип SIEM.	Решението може да създава, съхранява и предоставя log файлове към трети решения, използвайки Syslog протокол, например за предоставяне на информация на решения от тип SIEM. Източник: ENDPOINT SECURITY SERVER SYSTEM ADMINISTRATION GUIDE RELEASE 5.0 Страница 316
REQ.31.	Решението трябва да позволява интеграция с решения тип SIEM за автоматична подмяна на заявки и информация, така че да се намали необходимото време за разследване на атака.	Решението позволява интеграция с решения тип SIEM за автоматична подмяна на заявки и информация, така че да се намали необходимото време за разследване на атака. Източник: ENDPOINT SECURITY SERVER SYSTEM ADMINISTRATION GUIDE RELEASE 5.0 Страница 316
REQ.32.	В случаите когато агента не може да установи комуникация с устройстовто-контролер, агента трябва да продължи нормалната си работа и да изпрати събраната информация към контролера, когато комуникацията се установи отново.	В случаите когато агентът не може да установи комуникация с устройстовото-контролер, агентът може да продължи нормалната си работа и да изпрати събраната информация към контролера, когато комуникацията се установи отново. Източник: ENDPOINT SECURITY AGENT ADMINISTRATION GUIDE RELEASE 32.30.0 Страница 17
REQ.33.	Решението трябва да може да се интегрира с подсистемата за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения за корелация на събития през подсистемата за централизирано управление.	Решението може да се интегрира с подсистемата за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения за корелация на събития през подсистемата за централизирано управление.

		Източник: ENDPOINT SECURITY SERVER SYSTEM ADMINISTRATION GUIDE RELEASE 5.0 Страница 309
Хардуерни изисквания – 2 броя основен и DMZ		**Предложение: 1 брой основно хардуерно устройство с вграден софтуер FireEye HW-4502 HX с включена 5-годишна поддръжка и 1 брой DMZ хардуерно устройство с вграден софтуер FireEye HW-4502D HX DMZ с включена 5-годишна поддръжка**
REQ.34.	Устройството да може да управлява сигурността на до 100 000 крайни точки (максимален капацитет на скалируемост)	Устройството може да управлява сигурността на до 100 000 крайни точки https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/ep/ds-endpoint-security-specs.pdf **Table 2.** Physical appliance specifications. **Model Name** — **HX4502 or HX4502-D** **Maximum Endpoints Managed** — 100,000 **Form Factor** — 1U
REQ.35.	Устройството да е с максимална големина 1U	Устройството е с големина 1U https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/ep/ds-endpoint-security-specs.pdf **Table 2.** Physical appliance specifications. **Model Name** — **HX4502 or HX4502-D** **Maximum Endpoints Managed** — 100,000 **Form Factor** — 1U
REQ.36.	Устройството да разполага с ефективно място за съхранение на получените данни от крайните точки, минимално 8TB	Устройството разполага с 8TB ефективно място за съхранение на получените данни от крайните точки https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/ep/ds-endpoint-security-specs.pdf

REQ.37.	Устройството да разполага минимално със следните портове: 2x 1GigE BaseT, 1x IPMI, 2x USB3 (rear), 1x DB9 Serial, 1x VGA	Устройството разполага със следните портове: 2x 1GigE BaseT, 1x IPMI, 2x USB3 (rear), 1x DB9 Serial, 1x VGA https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/ep/ds-endpoint-security-specs.pdf
REQ.38.	Резервирано захранване – 1+1	Устройството разполага с резервирано захранване – 1+1 https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/ep/ds-endpoint-security-specs.pdf
REQ.39.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.	Устройството работи в изолиран режим, без Интернет свързаност. Устройството не изпраща данни към производителя за засечените заплахи в организацията. https://www.fireeye.com/company/legal.html
Гаранция и поддръжка:		**Предлагана гаранция и поддръжка от производителя:**
REQ.40.	Срок на хардуерната гаранция - минимум 5 (пет) години.	Срокът на хардуерната гаранция е 5 (пет) години.
REQ.41.	Срок на техническа поддържка – минимум 5 (пет) години.	Срокът на техническа поддръжка е 5 (пет) години.
REQ.42.	Получаване на нови версии на софтуера - минимум 5 (пет) години.	Новите версии на софтуера ще се получават 5 (пет) години.
REQ.43.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.	Обновяването на дефиниции и сигнатури е 5 (пет) години.

1.4.2. Подсистема за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения

Изискано от Възложителя	Предложено от участника
А.	**Б.**
Общи изисквания	

REQ.44.	Брой пощенски кутии: 8000	Предлаганата подсистема за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения е предназначена **за 8000 пощенски кутии.**
REQ.45.	Тип решение: 2 броя хардуер (High-Availability) с вграден софтуер и 5-годишна поддръжка, както и включен абонамент за 8000 софтуерни лицензи за анализиране на прикачени файлове и URL адреси в email съобщенията, също с 5-годишна поддръжка, 2 бр. 5-годишен абонамент за прилежащи услуги към хардуерните устройства	Предлаганата подсистема за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения включва: **2 броя хардуерни устройства (High-Availability) с вграден софтуер FireEye 8500EX-HW EMAIL MPS с включена 5-годишна поддръжка; абонамент за 8000 софтуерни лицензи за анализиране на прикачени файлове и URL адреси в email съобщенията FireEye Attach/URL engine-9999-5Y; 2 бр. 5-годишен абонамент за прилежащите услуги към хардуерните устройства FireEye DTI 8500 EX Off sub-5Y**
REQ.46.	Решението трябва да може да открива и идентифицира зловреден код, който е скрит и влиза в организацията чрез електронната поща, като трябва да се използват технологии и методи за засичане, които да не са базирани само на статичен анализ чрез дефиниции, статични списъци или правила, а да може да извършва и динамичен анализ и да открива непознати "zero-day" заплахи.	Решението може да открива и идентифицира зловреден код, който е скрит и влиза в организацията чрез електронната поща, като се използват технологии и методи за засичане, които не са базирани само на статичен анализ чрез дефиниции, статични списъци или правила, а може да извършва и динамичен анализ и открива непознати "zero-day" заплахи. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/fireeye-ex-series.pdf
REQ.47.	Решението трябва да се предоставя под формата на специализиран хардуер, като производителя трябва да е отговорен и да предостави лицензи за софтуер за поне 120	Решението се предоставя под формата на специализиран хардуер, като производителят е отговорен и предоставя лицензи за софтуер за поне 120 виртуални машини за анализ, с

	виртуални машини за анализ, с прилежащите им операционни системи и приложения.	прилежащите им операционни системи и приложения. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/fireeye-ex-series.pdf
REQ.48.	Решението трябва да притежава следните сертификати: Federal Information Processing Standards (FIPS) 140-2 и Common Criteria (CC).	Решението притежава следните сертификати: Federal Information Processing Standards (FIPS) 140-2 и Common Criteria (CC). https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/fireeye-ex-series.pdf Security Certifications | FIPS 140-2, CC NDPP v1.1 | FIPS 140-2, CC NDPP v1.1 | FIPS 140-2, CC NDPP v1.1
REQ.49.	Решението трябва да може да открива фишинг и spear-фишинг атаки. Трябва да може да анализира прикачени файлове и URL адреси в електронните съобщения, за да открива опити за компроментиране на системите на организацията.	Решението може да открива фишинг и spear-фишинг атаки, може да анализира прикачени файлове и URL адреси в електронните съобщения, като по този начин открива опити за компроментиране на системите на организацията. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/fireeye-ex-series.pdf
REQ.50.	Решението трябва да може да открива impersonation атаки (представяне с чужда самоличност). Трябва да се позволява конфигурирането на отношения между имена и email адреси, така че да се засичат опити за impersonation атаки, които копират имената или email адресите на потребителите.	Решението може да открива impersonation атаки (представяне с чужда самоличност). Позволява се конфигурирането на отношения между имена и email адреси, така че да се засичат опити за impersonation атаки, които копират имената или email адресите на потребителите. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 **Страница 173**
REQ.51.	Решението трябва да може да засича зловреден код с голяма точност, с изключително малък процент на грешни	Решението може да засича зловреден код с голяма точност, с изключително малък процент на грешни показания. Може да открива с точност

[redacted] [redacted] [redacted] [redacted]

	показания. Трябва да може да се открива с точност зловреден код, независимо от MIME тип, тип на разширение (extension) и независимо дали са използвани техники за скриване или архивиране на съдържанието на електронните съобщения.	зловреден код, независимо от MIME тип, тип на разширение (extension) и независимо, дали са използвани техники за скриване или архивиране на съдържанието на електронните съобщения. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 123, 125, 129, 130
REQ.52.	Решението трябва да може да поставя в карантина email съобщения, които съдържат URL адреси в тялото си, съдържат MS Office документи, PDF документи, архиви и HTML файлове, замаскирани JAVA скриптове, замаскирани, съкратени или пренасочващи URL адреси.	Решението може да поставя в карантина email съобщения, които съдържат URL адреси в тялото си, съдържат MS Office документи, PDF документи, архиви и HTML файлове, замаскирани JAVA скриптове, замаскирани, съкратени или пренасочващи URL адреси. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 443-444
REQ.53.	Решението трябва да може да разпознава заплахи като извършва локален анализ, без да е необходимо да изпраща файлове, проби от зловреден код или изпълним код извън организацията или към облачно-базирани платформи за анализ.	Решението може да разпознава заплахи като извършва локален анализ, без да е необходимо да изпраща файлове, проби от зловреден код или изпълним код извън организацията или към облачно-базирани платформи за анализ. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/fireeye-ex-series.pdf
REQ.54.	Решението трябва да може да анализира множество типове файлове, използвайки различни приложения и техни версии за анализа, съответно за разширения (минимално): exe, dll, pdf, pub, doc, docx, xls, xlsx, js, gif, jpeg, png, tiff, swf, eml, mov, qt, mp4,	Решението може да анализира множество типове файлове, използвайки различни приложения и техни версии за анализа, съответно за разширения (минимално): exe, dll, pdf, pub, doc, docx, xls, xlsx, js, gif, jpeg, png, tiff, swf, eml, mov, qt, mp4, jpg, mp3, asf, ico, htm, hta, url, rm, com, vcf, ppt, rtf, chm, hlp.

<table>
<tr><td></td><td>jpg, mp3, asf, ico, htm, hta, url, rm, com, vcf, ppt, rtf, chm, hlp.</td><td>Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4

Страница 54

Email Security – Server Edition User Guide CHAPTER 2: System Configuration

<table><tr><th>Starts With</th><th>File Types</th></tr><tr><td>Numeral</td><td>3gp, 7zip</td></tr><tr><td>A</td><td>a3x, ace, acrobatsecuritysettings, ahk, alz, apk, app, applet, arj, asf, au3, avi</td></tr><tr><td>B</td><td>bat, bz2</td></tr><tr><td>C</td><td>cab, cdf, chm, cmd, com, cpl, csv</td></tr><tr><td>D</td><td>dll, dmg, doc, docm, docx, dual, dylib</td></tr><tr><td>E</td><td>eeml, eg, ehdr, elf, eml, empty, exe</td></tr><tr><td>F</td><td>fdf, flv</td></tr><tr><td>G</td><td>gsv, gif, gz</td></tr><tr><td>H</td><td>hlp, html, hta, htm, hwp, hwt</td></tr><tr><td>I</td><td>ico</td></tr><tr><td>J</td><td>jar, jpeg, jpg, js, jsp, jtd</td></tr><tr><td>L</td><td>lnk, lzh</td></tr><tr><td>M</td><td>mach-o, mht, mhtml, midi, mov, mp3, mp4, mpg, mpkg, msg, msi, mso</td></tr><tr><td>O</td><td>one</td></tr><tr><td>P</td><td>pdf, php, pkg, pl, png, pps, ppsx, ppt, pptx, psl, pub, py</td></tr><tr><td>Q</td><td>qt</td></tr><tr><td>R</td><td>rar, rb, rm, rmi, rtf</td></tr><tr><td>S</td><td>scf, sct, sh, swf</td></tr><tr><td>T</td><td>tiff, tmf</td></tr><tr><td>U</td><td>umk, url, url-applet, uue</td></tr><tr><td>V</td><td>vbs, vcf, vcs</td></tr><tr><td>W</td><td>wav, war, wma, wsf</td></tr><tr><td>X</td><td>xdp, xls, xlsx, xml, xor, xps, xsl</td></tr><tr><td>Z</td><td>zip</td></tr></table></td></tr>
<tr><td>REQ.55.</td><td>Решението трябва да може да извлича и анализира вмъкнати файлове в документи, като например pdf, rtf или MS Office документи.</td><td>Решението може да извлича и анализира вмъкнати файлове в документи, като например pdf, rtf или MS Office документи.

Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4

Страници: 85-86</td></tr>
<tr><td>REQ.56.</td><td>Решението трябва да може да поставя в карантина и да алармира за криптирани MS Office документи.</td><td>Решението може да поставя в карантина и да алармира за криптирани MS Office документи.

This example shows the current riskware detection custom policy rule configuration.
hostname (config) # show analysis riskware policy rules
<table><tr><th>Rule ID</th><th>Rule</th><th>Alert Only</th><th>Quarantine</th></tr><tr><td>65000</td><td>Jar Files Delivered Via Email Attachment Or Link</td><td>Enabled</td><td>Enabled</td></tr><tr><td>65001</td><td>Encrypted MS Office Document</td><td>Disabled</td><td>Disabled</td></tr></table></td></tr>
</table>

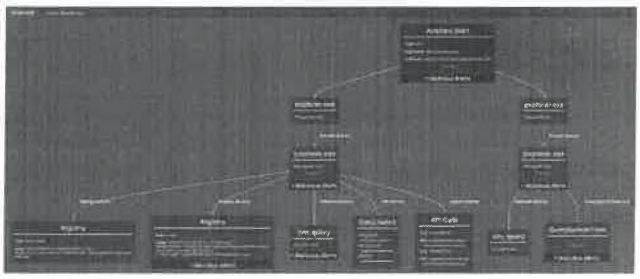
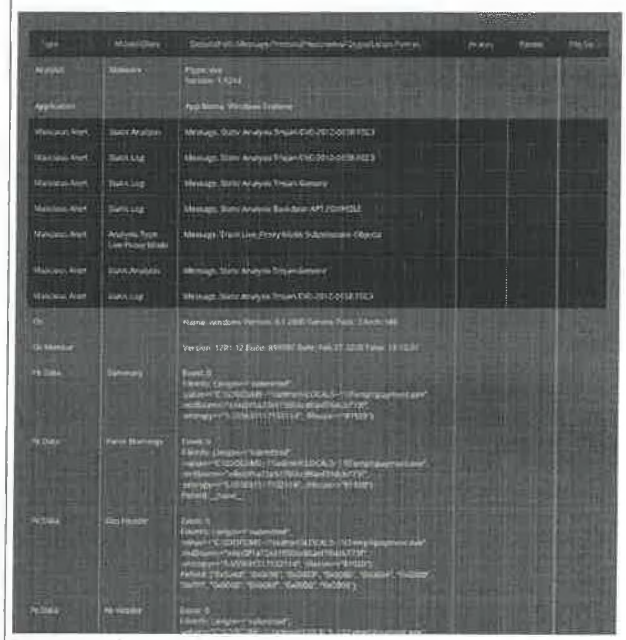
REQ.57.	Решението трябва да може да поставя в карантина и да алармира за прикачени MS Office документи, които съдържат макроси или имат вградени в тях документи, независимо от резултата от анализа.	Решението може да поставя в карантина и да алармира за прикачени MS Office документи, които съдържат макроси или имат вградени в тях документи, независимо от резултата от анализа. [redacted]
REQ.58.	Решението трябва да може да поставя в карантина и да алармира за електронни съобщения, които съдържат в себе си съкратени URL адреси.	Решението може да поставя в карантина и да алармира за електронни съобщения, които съдържат в себе си съкратени URL адреси. [redacted]
REQ.59.	За електронни съобщения, които съдържат URL адреси, които водят до сваляне на файлове, решението трябва да може да извлича и анализира въпросните файлове от URL адресите, като да може да се блокира съобщението ако файловете се окажат зловредни.	За електронни съобщения, които съдържат URL адреси, които водят до сваляне на файлове, решението може да извлича и анализира въпросните файлове от URL адресите, като може да се блокира съобщението, ако файловете се окажат зловредни. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страница 216
REQ.60.	Решението трябва да може да поставя в карантина и да алармира за електронни съобщения, които съдържат прикачени JAR файлове или съдържат URL адреси, които водят до JAR файлове.	Решението може да поставя в карантина и да алармира за електронни съобщения, които съдържат прикачени JAR файлове или съдържат URL адреси, които водят до JAR файлове.

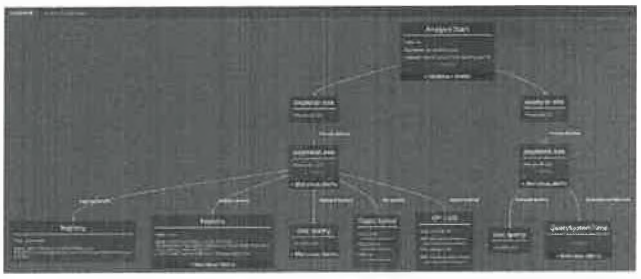
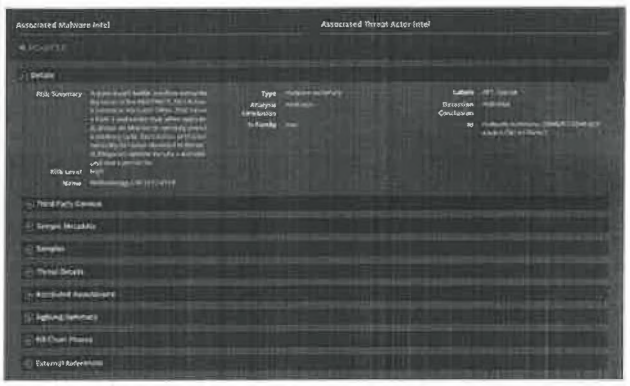
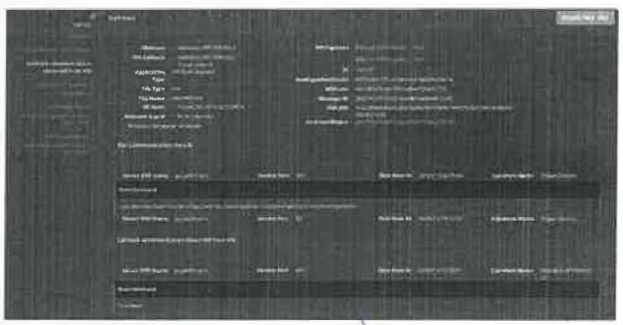
		Email Security – Server Edition User Guide CHAPTER 2: System Configuration Starts With: File Types Numeral: 3gp, 7zip A: a3x, ace, acrobatsecuritysettings, alik, alz, apk, app, applet, arj, asf, au3, avi B: bat, bz2 C: cab, cdf, chm, cmd, com, com1, csv D: dll, dmg, doc, docm, docx, dual, dylib E: eeml, eg, ehdr, elf, eml, empty, exe F: f4f, flv G: gen, gif, gz H: hlp, html, hta, htm, hwp, hwt I: ico J: jar, jpeg, jpg, js, jsp, jtd L: lnk, lzh M: mach-o, mht, mhtml, midi, mov, mp3, mp4, mpg, mpkg, msg, msi, mso O: one P: pdf, plip, pkg, pl, png, pps, ppsx, ppt, pptx, psl, pub, py Q: qt R: rar, rb, rm, rmi, rtf S: scf, sct, sh, swf T: tiff, tnef U: unk, url, url-applet, uue V: vbs, vcf, vcs W: wav, war, wma, wsf X: xdp, xls, xlsx, xml, xor, xps, xsl Z: zip
REQ.61.	Решението трябва да може да извлича и анализира URL адреси от съдържанието на електронните съобщения и от секцията „Относно" на съобщенията, както и от прикачени PDF или MS Office документи.	Решението може да извлича и анализира URL адреси от съдържанието на електронните съобщения и от секцията „Относно" на съобщенията, както и от прикачени PDF или MS Office документи. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страница 270
REQ.62.	Решението трябва да може да засича следните техники, които се използват от атакуващите хакери, за да подмамят потребителите да достъпят конкретни URL адреси: заместване на знак от адреса с друг (typosquatting), използване на линк към различен адрес от изображения (URL overlay).	Решението може да засича следните техники, които се използват от атакуващите хакери, за да подмамят потребителите да достъпят конкретни URL адреси: заместване на знак от адреса с друг (typosquatting), използване на линк към различен адрес от изображения (URL overlay).

		Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 502, 510
REQ.63.	Решението трябва да може да анализира URL адреси от тип ftp, http и https.	Решението може да анализира URL адреси от тип ftp, http и https. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 270, 306, 307
REQ.64.	Решението трябва да може да анализира base64 кодирани URL адреси.	Решението може да анализира base64 кодирани URL адреси. Източник: EX SERIES RELEASE NOTES RELEASE 8.1 Страница 7
REQ.65.	Решението трябва да анализира прикачени архиви тип 7Z, ZIP, LZH, RAR. Ако архивите са защитени с парола, решението да може автоматично да търси подходящи варианти за парола в съдържанието на електронното съобщение, в самите файлове-архиви или в прикачени изображения към съобщението чрез OCR технология.	Решението може да анализира прикачени архиви тип 7Z, ZIP, LZH, RAR. Ако архивите са защитени с парола, решението може автоматично да търси подходящи варианти за парола в съдържанието на електронното съобщение, в самите файлове-архиви или в прикачени изображения към съобщението чрез OCR технология. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 66-67, 77
REQ.66.	Решението трябва да може да извлича и анализира URL адреси от заключени с парола PDF или MS Office документи. Решението да може автоматично да търси подходящи варианти за парола в съдържанието на електронното съобщение или в прикачени изображения към съобщението чрез OCR	Решението може да извлича и анализира URL адреси от заключени с парола PDF или MS Office документи. Решението може автоматично да търси подходящи варианти за парола в съдържанието на електронното съобщение или в прикачени изображения към съобщението чрез OCR технология (изображения тип JPEG, PNG, BMP, TIFF).

	технология (изображения тип JPEG, PNG, BMP, TIFF).	Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 66-67, 77
REQ.67.	Решението трябва да може да анализира файлове не само чрез статичен анализ с дефиниции, но и чрез алгоритми за машинно обучение и динамичен анализ тип sandbox.	Решението може да анализира файлове не само чрез статичен анализ с дефиниции, но и чрез алгоритми за машинно обучение и динамичен анализ тип sandbox. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 491
REQ.68.	Решението трябва да може да анализира (във виртуалните машини за динамичен анализ) сваленитe файлове от заявки идващи от exploit атаки. Например, ако прикачен файл към електронно съобщение съдържа скрипт / макрос, който опитва да свали допълнителни файлове и съдържание, то решението трябва да може успешно да ги свали и анализира, за да се открият и предотвратят атаки, които се развиват на няколко фази.	Решението може да анализира (във виртуалните машини за динамичен анализ) сваленитe файлове от заявки, идващи от exploit атаки. Например, ако прикачен файл към електронно съобщение съдържа скрипт / макрос, който опитва да свали допълнителни файлове и съдържание, то решението може успешно да ги свали и анализира, за да се открият и предотвратят атаки, които се развиват на няколко фази. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 234
REQ.69.	Решението трябва да може да открива с много висока точност, с възможно най-малко грешни показания, файлове, които след анализ на поведението се държат по подобие на зловреден код: поведение, което опитва да избегне засичане, инсталиране на нежелани програми, промени по системните настройки, намаляване на цялостната производителност	Решението може да открива с много висока точност, с възможно най-малко грешни показания, файлове, които след анализ на поведението се държат по подобие на зловреден код: поведение, което опитва да избегне засичане, инсталиране на нежелани програми, промени по системните настройки, намаляване на цялостната производителност на системата, потенциално

	на системата, потенциално нежелани програми (PUP), потенциално нежелани приложения (PUA), adware процеси, инструменти, които често се използват от атакуващи хакери.	нежелани програми (PUP), потенциално нежелани приложения (PUA), adware процеси, инструменти, които често се използват от атакуващи хакери. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 146-147
REQ.70.	По време на анализа във виртуалните машини, решението трябва да може да извлича и анализира URL адресите в паметта на машините.	По време на анализа във виртуалните машини, решението може да извлича и анализира URL адресите в паметта на машините. Източник: FireEye Guest Images release 17.0109
REQ.71.	Решението трябва да може да засича ransomware криптиращи атаки и атаки предназначени за POS терминали.	Решението може да засича ransomware криптиращи атаки и атаки, предназначени за POS терминали. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 234-235 Източник: FireEye Guest Images release 16.0901
REQ.72.	Решението трябва да може да алармира за зловредни процеси (файлове и URL адреси), които не са били засечени в първоначалните 24 часа, а на по-късен етап е установено, че са зловредни.	Решението може да алармира за зловредни процеси (файлове и URL адреси), които не са били засечени в първоначалните 24 часа, а на по-късен етап е установено, че са зловредни. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 495
REQ.73.	Решението трябва да предоставя цялостна информация след анализ на зловреден код. Информацията трябва да включва използвани уеб линкове за атаката, хеш суми на сваленитe	Решението предоставя цялостна информация след анализ на зловреден код. Информацията включва използвани уеб линкове за атаката, хеш суми на сваленитe файлове, цялостен одит на

	файлове, цялостен одит на действията по системите (променени ключове от регистрите, създаване и изпълнение на файлове, промяна в автоматичните настройки и параметрите за стартиране на приложения), както и да се предоставя информация за хронологичния ред от събития, свързани с атаката, започващи от фазата на уеб-експлоатация и първоначално проникване, до свалянето на код, установяване на контрол над системите и опитите за извличане на данни извън организацията.	действията по системите (променени ключове от регистрите, създаване и изпълнение на файлове, промяна в автоматичните настройки и параметрите за стартиране на приложения), както и предоставя информация за хронологичния ред от събития, свързани с атаката, започващи от фазата на уеб-експлоатация и първоначално проникване, до свалянето на код, установяване на контрол над системите и опитите за извличане на данни извън организацията.  
REQ.74.	Решението трябва да предоставя следствена информация след динамичния анализ на файлове, представена в графичен вид, изобразявайки процеси, достъпи до паметта, промени по файлове и регистри, качени DLL	Решението предоставя следствена информация след динамичния анализ на файлове, представена в графичен вид, изобразявайки процеси, достъпи до паметта, промени по файлове и регистри,

	библиотеки, инжектиране на код, heap spraying процеси, mutex процеси.	качени DLL библиотеки, инжектиране на код, heap spraying процеси, mutex процеси. 
REQ.75.	Решението трябва да може да предоставя, където е възможно, информация за атакуващата хакерска групировка и възможни стъпки за отстраняване на щетите (remediation) след дадена атака.	Решението може да предоставя, където е възможно, информация за атакуващата хакерска групировка и възможни стъпки за отстраняване на щетите (remediation) след дадена атака. 
REQ.76.	Ако при анализ на зловреден прикачен файл се установят опити за мрежови свързвания извън организацията от него, решението трябва да сигнализира и за тях при вдигането на съответната аларма.	Ако при анализ на зловреден прикачен файл се установят опити за мрежови свързвания извън организацията от него, решението може да сигнализира и за тях при вдигането на съответната аларма. 

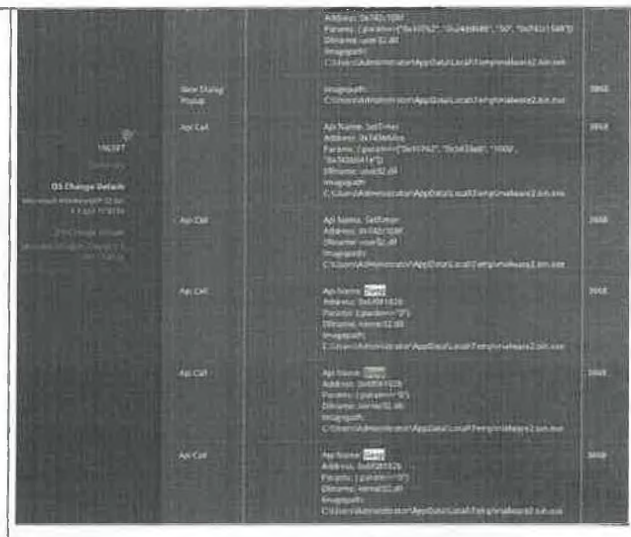
REQ.77.	Решението трябва да може да предоставя screenshot на зареден в браузър зловреден URL адрес по време на анализа му, за да се добие визуална представа за съдържанието на URL адреса.	Решението може да предоставя screenshot на зареден в браузър зловреден URL адрес по време на анализа му, за да се добие визуална представа за съдържанието на URL адреса. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 442
REQ.78.	Решението трябва да може да прави корелация на електронни съобщения със сходни характеристики, като например с еднакви прикачени файлове, еднакви заглавни части, еднакви изпращачи и т.н. и да може да ги групира като email кампании.	Решението може да прави корелация на електронни съобщения със сходни характеристики, като например с еднакви прикачени файлове, еднакви заглавни части, еднакви изпращачи и т.н. и да може да ги групира като email кампании. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 470
REQ.79.	Решението трябва да може да прави анализ на входящи електронни съобщения, използвайки едновременно множество виртуални машини с различни операционни системи, като например минимално Windows XP, 7 или Mac OSX, с различни версии на Service Pack, на 32 и на 64 битови платформи.	Решението може да прави анализ на входящи електронни съобщения, използвайки едновременно множество виртуални машини с различни операционни системи, като например минимално Windows XP, 7 или Mac OSX, с различни версии на Service Pack, на 32 и на 64 битови платформи.
REQ.80.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и	Решението не използва комерсиален хипервайзор, който може да бъде засечен и избегнат от

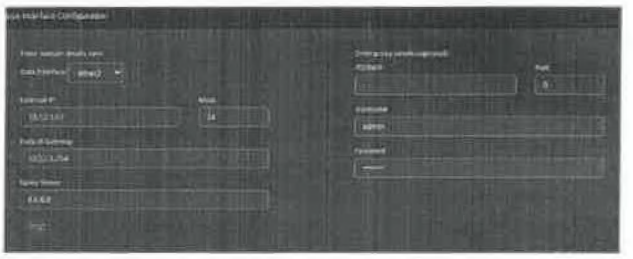
	избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н. Решението трябва да използва собствен, специално изграден хипервайзор.	зловредния код, като например Vmware, Hyper-V, KMV, Citrix и т.н. Решението използва собствен, специално изграден хипервайзор. https://www.fireeye.com/content/dam/fireeye-www/company/events/infosec/france-tech-track-summit.pdf Страница 22
REQ.81.	Решението трябва да позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите трябва да могат да променят поне следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, използваният Outlook акаунт, езика на машината, времевата зона на машината.	Решението позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите могат да променят следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, използвания Outlook акаунт, езика на машината, времевата зона на машината. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 46-49

4. Enter one or more of the following configuration settings:

Parameter Group	Fields	Description	Response
User Name	–	Name of user	–
Domain Name	–	Name of domain	–
Host Name	–	Name of host	–
Computer Name	–	Name of computer	–
Home Directory	Home Drive	Name of a home drive	–
Windows Recent Files	File Path	List of file path names	Enter a file path name. For example, c:\windows\sample.txt.
Office Recent Files	Office Recent File Path	Name of file path	Enter a file path name. For example, c:\office\recent. txt.
Browser History	Browser History URL	List of URLs	Enter a URL. For example, http://www.google.com.
Honey Credentials	Type	System or Browser	Enter a honey credential that includes type (system or browser), user name, and password. For example, browser:john.smith: honey_password123.
	User Name	Name of user	–
	Password	Password for authenticating honey credential	–
Honey Files	Honey File	List of honey file path names	–

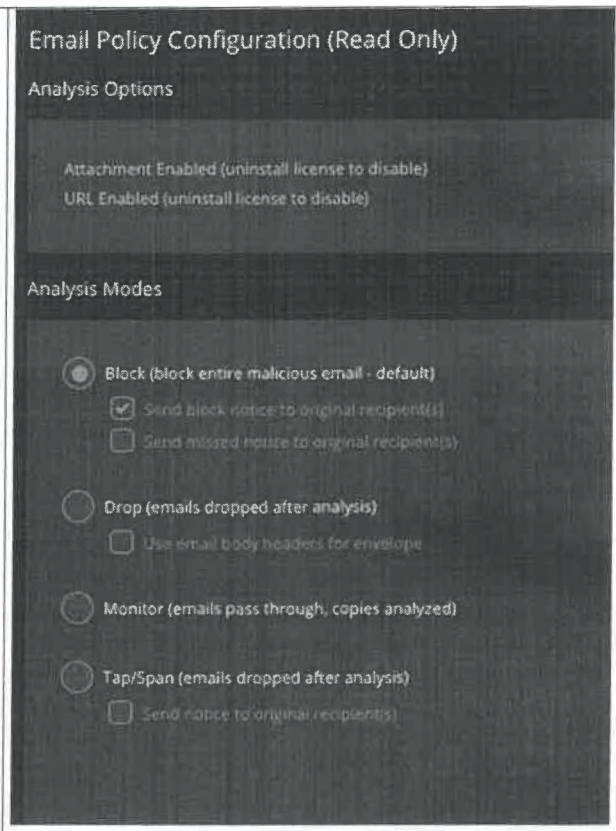
		<table><tr><th>Parameter Group</th><th>Fields</th><th>Description</th><th>Response</th></tr><tr><td>Honey Directories</td><td>Honey Directory</td><td>List of honey directory path names</td><td>–</td></tr><tr><td>DNS Cache Entries</td><td>Host Name</td><td>Host name entry</td><td>–</td></tr><tr><td></td><td>IP</td><td>IPv4 address</td><td>–</td></tr><tr><td>Host File Entries</td><td>Host Name</td><td>Host name entry</td><td>–</td></tr><tr><td></td><td>IP</td><td>IPv4 address</td><td>–</td></tr><tr><td>Outlook Account</td><td>User Name</td><td>Outlook user name</td><td>–</td></tr><tr><td></td><td>Password</td><td>Password for authenticating Outlook account</td><td>–</td></tr><tr><td>FTP Account</td><td>Host Name</td><td>FTP host name</td><td>–</td></tr><tr><td></td><td>User Name</td><td>FTP user name</td><td>–</td></tr><tr><td></td><td>Password</td><td>Password for authenticating FTP account</td><td>–</td></tr><tr><td>Skype User Account</td><td>User Name</td><td>Skype user name</td><td>–</td></tr><tr><td></td><td>Password</td><td>Password for authenticating Skype account</td><td>–</td></tr><tr><td>Language</td><td>Language</td><td>Preferred language</td><td>–</td></tr><tr><td>Time Zone</td><td>Time Zone</td><td>Preferred time zone</td><td>–</td></tr></table>
REQ.82.	Решението трябва да може да засича опити за използване на функциите за приспиване (sleep) на операционните системи от зловредния код и да може да забързва времето на виртуалните машини за анализ, за да принуди изпълнението на зловредния код.	Решението може да засича опити за използване на функциите за приспиване (sleep) на операционните системи от зловредния код и може да забързва времето на виртуалните машини за анализ, за да принуди изпълнението на зловредния код.

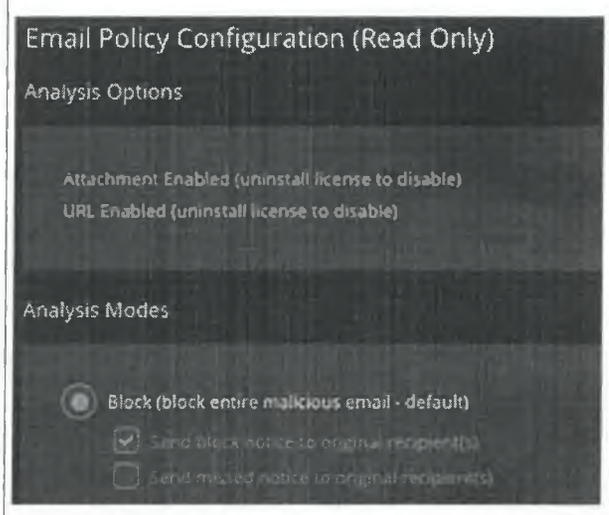
		
REQ.83.	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques), например използване на ping команди, проверка на домейн, проверка на отметки в наличните браузъри.	Решението може да се справя с техники за избягване от засичане (evasion techniques), например използване на ping команди, проверка на домейн, проверка на отметки в наличните браузъри. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 46-49
REQ.84.	Email решението трябва да поддържа inline MTA режим на работа.	Email решението поддържа inline MTA режим на работа. Източник: EMAIL SECURITY — SERVER EDITION SYSTEM ADMINISTRATION GUIDE RELEASE 8.4.2 Страници: 18, 20
REQ.85.	Email решението трябва да поддържа SPAN/TAP режим на работа.	Email решението поддържа SPAN/TAP режим на работа. Източник: EMAIL SECURITY — SERVER EDITION SYSTEM ADMINISTRATION GUIDE RELEASE 8.4.2 Страници: 18, 20
REQ.86.	Email решението трябва да поддържа BCC режим на работа.	Email решението поддържа BCC режим на работа.

		Източник: EMAIL SECURITY — SERVER EDITION SYSTEM ADMINISTRATION GUIDE RELEASE 8.4.2 Страници: 18, 20
REQ.87.	Решението трябва да позволява (по избор от администратор) извършване на динамичен анализ на файлове във виртуалните машини, както в режим на изолация (без да е необходима свързаност с Интернет), така и с позволено мрежово свързване от виртуалните машини, за да се добие цялостен анализ на зловредния код.	Решението позволява (по избор от администратор) извършване на динамичен анализ на файлове във виртуалните машини, както в режим на изолация (без да е необходима свързаност с Интернет), така и с позволено мрежово свързване от виртуалните машини, за да се добие цялостен анализ на зловредния код. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 233, 236, 242, 245
REQ.88.	Решението трябва да използва специално заделен мрежови интерфейс когато е пуснато в „жив" режим, за да се избегне допускането на зловреден мрежови трафик към реалната вътрешна мрежа на организацията; Мрежовия интерфейс трябва да позволява на зловредния код да достъпва външни хакерски командни сървъри и да сваля всички допълнителни модули и артефакти, които са му необходими, за да се изпълни изцяло за анализ.	Решението използва специално заделен мрежови интерфейс, когато е пуснато в „жив" режим, за да се избегне допускането на зловреден мрежови трафик към реалната вътрешна мрежа на организацията; Мрежовият интерфейс позволява на зловредния код да достъпва външни хакерски командни сървъри и да сваля всички допълнителни модули и артефакти, които са му необходими, за да се изпълни изцяло за анализ. 
REQ.89.	Решението трябва да може да симулира потребителски действия, за да изпълни зловреден код изискващ подобни действия, като	Решението може да симулира потребителски действия, за да изпълни зловреден код, изискващ подобни действия, като например щракане с мишката или конфигуриране на конкретни данни.

	например щракане с мишката или конфигуриране на конкретни данни.	https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/pf/file/fireeye-hot-knives-through-butter.pdf
REQ.90.	Цялостния анализ на електронно съобщение не трябва да отнема повече от 10 минути.	Цялостният анализ на електронно съобщение не отнема повече от 10 минути. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 267
REQ.91.	Решението трябва да позволява на администраторите да конфигурират максималното време за анализ на електронните съобщения.	Решението позволява на администраторите да конфигурират максималното време за анализ на електронните съобщения. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 267
REQ.92.	Решението трябва да позволява използването на YARA правила и да позволява конфигурирането на автоматични аларми или поставяне в карантина ако дадено съобщение отговаря на зададените YARA правила.	Решението позволява използването на YARA правила и позволява конфигурирането на автоматични аларми или поставяне в карантина, ако дадено съобщение отговаря на зададените YARA правила. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 52
REQ.93.	Решението трябва да може да засича и отчита опити за мрежова комуникация с Интернет от виртуалните машини по време на анализа.	Решението може да засича и отчита опити за мрежова комуникация с Интернет от виртуалните машини по време на анализа.

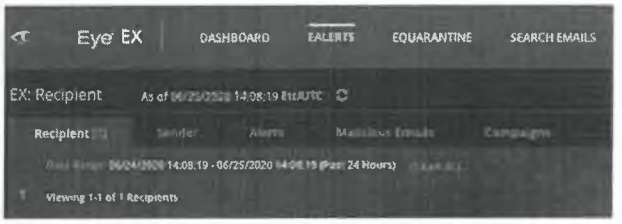
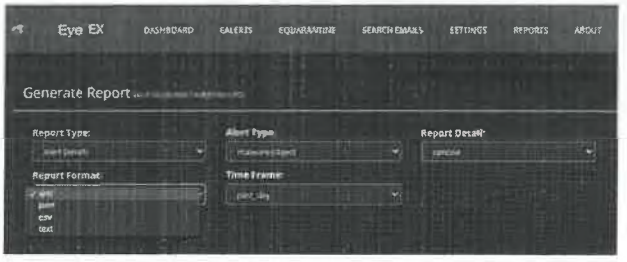
REQ.94.	Решението трябва да позволява на администраторите да посочват и обвързват с кои приложения да се стартират различните файлови разширения по време на анализа във виртуалните машини.	Решението позволява на администраторите да посочват и обвързват с кои приложения да се стартират различните файлови разширения по време на анализа във виртуалните машини. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 81
REQ.95.	Решението трябва да може да се имплементира в различни режими, както „Inline", на пътя на трафика, с възможност за блокиране, така и „Out-Of-Band", където да се анализират копия на електронните съобщения.	Решението може да се имплементира в различни режими, както „Inline", на пътя на трафика, с възможност за блокиране, така и „Out-Of-Band", където се анализират копия на електронните съобщения.

		
REQ.96.	Решението трябва да може да работи в напълно изолирана среда, без връзка с Интернет.	Решението може да работи в напълно изолирана среда, без връзка с Интернет. https://www.fireeye.com/company/legal.html
REQ.97.	Решението трябва да може да изпраща автоматични известия чрез Syslog, HTTP, SNMP и SMTP протоколи.	Решението може да изпраща автоматични известия чрез Syslog, HTTP, SNMP и SMTP протоколи. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 343
REQ.98.	Решението трябва да поддържа криптирана TLS комуникация (opportunistic или imposed), за да се запази конфиденциалността на електронните съобщения.	Решението поддържа криптирана TLS комуникация (opportunistic или imposed), за да се запази конфиденциалността на електронните съобщения. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 201

		Field — **Description** None — Enabled in both receiving mode and default delivery mode, no connections are configured with TLS. Opportunistic — Enabled in receiving mode, the connection accepts emails that are either TLS-encrypted or not TLS-encrypted based on the upstream configuration. Enabled in default delivery mode, emails are delivered over connections that are either TLS-encrypted or not TLS-encrypted to the remote MTA. Mandatory — Enabled in both receiving mode and default delivery mode. TLS configuration is required for all connections. Enabled in receiving mode, if TLS is not supported on the upstream device, emails are not accepted and they remain on the upstream device until the connection accepts emails that are not TLS-encrypted. Enabled in default delivery mode, if the next-hop does not support TLS, emails are not delivered and remain deferred on the appliance for five days or until TLS is supported in the remote MTA. Verify — Enabled in default delivery mode, validation of the next-hop MTA server certificate and the imported certificate authority (CA) are required before the TLS connection is established. For information about TLS certificate configuration and TLS CA configuration, see the *Email Security — Server Edition System Administration Guide*.
REQ.99.	Решението трябва да може да изпраща автоматични известия когато блокира или постави в карантина дадено електронно email съобщение.	Решението може да изпраща автоматични известия, когато блокира или постави в карантина дадено електронно email съобщение. 
REQ.100	Решението трябва да позволява конфигурирането на обема на заделеното място за карантина на съобщенията и да може да изпраща автоматични известия когато заделеното пространство се запълни до определен процент.	Решението позволява конфигурирането на обема на заделеното място за карантина на съобщенията и може да изпраща автоматични известия, когато заделеното пространство се запълни до определен процент.

REQ.101.	Решението трябва да позволява използването на прокси с оторизация за свързване със сървър за обновления на софтуера и информацията за нови заплахи.	Решението позволява използването на прокси с оторизация за свързване със сървър за обновления на софтуера и информацията за нови заплахи. Източник: EMAIL SECURITY — SERVER EDITION SYSTEM ADMINISTRATION GUIDE RELEASE 8.4.2 Страници: 111
REQ.102.	Решението трябва да позволява администрация чрез уеб-базирана конзола, без да се изисква инсталирането на допълнителен софтуер за достъпването ѝ.	Решението позволява администрация чрез уеб-базирана конзола, без да се изисква инсталирането на допълнителен софтуер за достъпването ѝ. Източник: EMAIL SECURITY — SERVER EDITION SYSTEM ADMINISTRATION GUIDE RELEASE 8.4.2 Страници: 31
REQ.103.	Решението трябва да позволява конфигурирането на ACL списъци, за да се ограничи достъпа до интерфейса за централизирано управление.	Решението позволява конфигурирането на ACL списъци, за да се ограничи достъпа до интерфейса за централизирано управление. Източник: EMAIL SECURITY — SERVER EDITION SYSTEM ADMINISTRATION GUIDE RELEASE 8.4.2 Страници: 194
REQ.104.	Решението трябва да използва криптирана комуникация между администраторите и конзолата за централизирано управление. Трябва да позволява вмъкването на собствени дигитални сертификати на организацията.	Решението използва криптирана комуникация между администраторите и конзолата за централизирано управление. Решението позволява вмъкването на собствени дигитални сертификати на организацията. Източник: EMAIL SECURITY — SERVER EDITION SYSTEM ADMINISTRATION GUIDE RELEASE 8.4.2 Страници: 148-149

REQ.105.	Решението трябва да позволява локално конфигуриране или чрез синхронизация с NTP сървър на използваните време и часова зона.	Решението позволява локално конфигуриране или чрез синхронизация с NTP сървър на използваните време и часова зона. Източник: EMAIL SECURITY — SERVER EDITION SYSTEM ADMINISTRATION GUIDE RELEASE 8.4.2 Страници: 169
REQ.106.	Решението трябва да поддържа ролево-базиран достъп до конзолата за управление. Да могат да се задават различни профили и права (администратор, оператор, одитор и т.н.), като да се задават кои отчети, аларми и информация могат да виждат в конзолата за управление.	Решението поддържа ролево-базиран достъп до конзолата за управление. Могат да се задават различни профили и права (администратор, оператор, одитор и т.н.), като се задават кои отчети, аларми и информация могат да виждат в конзолата за управление. Източник: SYSTEM SECURITY SYSTEM SECURITY GUIDE RELEASE 2019.4 Страници: 29, 161
REQ.107.	Решението трябва да поддържа LDAP, TACACS + или RADIUS методи за вписване на потребителите.	Решението поддържа LDAP, TACACS + и RADIUS методи за вписване на потребителите. Източник: SYSTEM SECURITY SYSTEM SECURITY GUIDE RELEASE 2019.4 Страници: 57, 61, 63, 66, 67
REQ.108.	Решението трябва да може да изпраща известия за собственото си здраве и процеси и генерираните отчети, чрез SMTP, SNMP и Syslog протоколи.	Решението може да изпраща известия за собственото си здраве и процеси и генерираните отчети, чрез SMTP, SNMP и Syslog протоколи. Източник: SYSTEM SECURITY SYSTEM SECURITY GUIDE RELEASE 2019.4 Страници: 155, 159, 223, 271
REQ.109.	Решението трябва да позволява извличането на аларми и отчети за активност на зловреден код в PDF формат.	Решението позволява извличането на аларми и отчети за активност на зловреден код в PDF формат.

		Източник: EMAIL SECURITY — SERVER EDITION SYSTEM ADMINISTRATION GUIDE RELEASE 8.4.2 **Страници: 34**
REQ.110.	Решението трябва да позволява групирането на аларми за зловредни email съобщения по поне следните критерии: по изпращачи, по получатели, по видове вдигнати аларми, по email кампания.	Решението позволява групирането на аларми за зловредни email съобщения по следните критерии: по изпращачи, по получатели, по видове вдигнати аларми, по email кампания. 
REQ.111.	Решението трябва да позволява генерирането на отчети в PDF или в CSV формат, според типа информация в тях: вдигнати аларми и техните детайли, тип инфекция, обобщителна информация за предоставяне пред ръководните органи на организацията, списък с достъпените сървъри при callback комуникация и други.	Решението позволява генерирането на отчети в PDF или в CSV формат, според типа информация в тях: вдигнати аларми и техните детайли, тип инфекция, обобщителна информация за предоставяне пред ръководните органи на организацията, списък с достъпените сървъри при callback комуникация и други. Източник: EMAIL SECURITY — SERVER EDITION SYSTEM ADMINISTRATION GUIDE RELEASE 8.4.2 **Страници: 519-522** 

		Print PDF Standard Processing Time Extra Processing Time Heavy Processing Time
REQ.112.	Решението трябва да предоставя опция да получава и изпраща обекти за анализ, когато бъде достигнат зададен лимит на капацитета на обработваните обекти от решението, към предварително зададен локално-разположен клъстър или към специализирани хардуерни устройства за балансиране на производителността.	Решението предоставя опция да получава и изпраща обекти за анализ, когато бъде достигнат зададен лимит на капацитета на обработваните обекти от решението, към предварително зададен локално-разположен клъстър или към специализирани хардуерни устройства за балансиране на производителността. Източник: EMAIL SECURITY — SERVER EDITION SYSTEM ADMINISTRATION GUIDE RELEASE 8.4.2 Страници: 63
REQ.113.	Решението трябва да позволява извличането на метаданни от email съобщенията, минимално получател, прикачени файлове и вмъкнати URL адреси, като тези метаданни да могат да се изпращат към решение тип SIEM, чрез HTTP или чрез Rsyslog протокол.	Решението позволява извличането на метаданни от email съобщенията, минимално получател, прикачени файлове и вмъкнати URL адреси, като тези метаданни могат да се изпращат към решение тип SIEM, чрез HTTP или чрез Rsyslog протокол. Източник: EMAIL SECURITY — SERVER EDITION USER GUIDE RELEASE 8.4 Страници: 88
Хардуерни изисквания – 2 броя		**Предложение: 2 броя хардуерни устройства (High-Availability) с вграден софтуер FireEye 8500EX-HW EMAIL MPS с включена 5-годишна поддръжка**
REQ.114.	Устройството да може да анализира до 2650 уникални прикачени файлове към email съобщения в час	Устройството може да анализира до 2650 уникални прикачени файлове към email съобщения в час.

		https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/fireeye-ex-series.pdf Table 1. Technical specifications EX 3500 / EX 5500 / EX 8500 Performance* / Up to 700 unique attachments per hour / Up to 1,900 unique attachments per hour / Up to 2,650 unique attachments per hour
REQ.115.	Устройството да може да анализира прикачени файлове и URL адреси в email съобщенията за 8000 пощенски кутии	Устройството може да анализира прикачени файлове и URL адреси в email съобщенията за 8000 пощенски кутии https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/fireeye-ex-series.pdf
REQ.116.	Устройството да е с максимална големина 2RU	Устройството е с големина 2RU https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/fireeye-ex-series.pdf
REQ.117.	Устройството да разполага минимално със следните портове за наблюдение на мрежата: 2x 1GigE BaseT	Устройството разполага със следните портове за наблюдение на мрежата: 2x 1GigE BaseT https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/fireeye-ex-series.pdf
REQ.118.	Допълнителни портове: 2x 1GigE BaseT портове за управление, сериен порт, 4x Type A USB, IPMI, VGA	Устройството разполага със следните допълнителни портове: 2x 1GigE BaseT портове за управление, сериен порт, 4x Type A USB, IPMI, VGA https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/fireeye-ex-series.pdf
REQ.119.	Резервирано захранване – 1+1	Устройството разполага с резервирано захранване – 1+1 https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/email/fireeye-ex-series.pdf
REQ.120.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не	Устройството работи в изолиран режим, без Интернет свързаност. Устройството не изпраща

	изпраща данни към производителя за засечените заплахи в организацията.	данни към производителя за засечените заплахи в организацията. https://www.fireeye.com/company/legal.html
Гаранция и поддръжка:		**Предлагана гаранция и поддръжка от производителя:**
REQ.121.	Срок на хардуерната гаранция - минимум 5 (пет) години.	Срокът на хардуерната гаранция е 5 (пет) години.
REQ.122.	Срок на техническа поддържка – минимум 5 (пет) години.	Срокът на техническа поддръжка е 5 (пет) години.
REQ.123.	Получаване на нови версии на софтуера - минимум 5 (пет) години.	Новите версии на софтуера ще се получават 5 (пет) години.
REQ.124.	Обновяване на дефиниции и сигнатури – минимум 5 (пет) години.	Обновяването на дефиниции и сигнатури е 5 (пет) години.

1.4.3. Подсистема за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво

Изискано от Възложителя		**Предложено от участника**
А.		**Б.**
Общи изисквания		
REQ.125.	Тип решение: 2 броя хардуер (High-Availability) с вграден софтуер и 5-годишна поддръжка, с добавени 2 броя разширителни модули тип 1G-10G BASE-LX/LR FIBER, 2 бр. 5-годишен абонамент за прилежащи услуги към хардуерните устройства	Предлаганата подсистема за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво включва: **2 броя хардуерни устройства (High-Availability) с вграден софтуер FireEye HW-NX 5500 с включена 5-годишна поддръжка; 2 броя разширителни модули от производителя FireEye тип 1G-10G BASE-LX/LR FIBER; 2 бр. 5-годишен абонамент FireEye DTI NX 5500 Off-5Y за прилежащи услуги към хардуерните устройства**

REQ.126.	Предложеното решение трябва да може да инспектира и блокира зловреден мрежови трафик като да се поставя на пътя на трафика в inline режим или в „out-of-band" режим, като да може да работи независимо от останалото мрежово оборудване в инфраструктурата.	Предложеното решение може да инспектира и блокира зловреден мрежови трафик като се поставя на пътя на трафика в inline режим или в „out-of-band" режим, като може да работи независимо от останалото мрежово оборудване в инфраструктурата. Източник: NX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 18
REQ.127.	Решението трябва да притежава следните сертификати: Federal Information Processing Standards (FIPS) 140-2 и Common Criteria (CC).	Решението притежава сертификатите Federal Information Processing Standards (FIPS) 140-2 и Common Criteria (CC). https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.128.	Решението да поддържа режим на работа с висока достъпност - high availability (HA), от типа active-active.	Решението поддържа режим на работа с висока достъпност - high availability (HA), от типа active-active. Източник: NX SERIES HIGH AVAILABILITY GUIDE RELEASE 8.2 Страници: 9
REQ.129.	Решението трябва да може да функционира независимо от което и да е друго мрежово устройство (например защитни стени, IDS/IPS устройства, security gateway устройства и т.н.). Решението трябва да е специализирано и да може да работи самостоятелно, като функциите му не трябва да са част от UTM или интегрирано решение за сигурност.	Решението може да функционира независимо от което и да е друго мрежово устройство (например защитни стени, IDS/IPS устройства, security gateway устройства и т.н.). Решението е специализирано и може да работи самостоятелно, като функциите му не са част от UTM или интегрирано решение за сигурност. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf

REQ.130	Предложеното решение трябва да предоставя предварително зададени правила за разпознаване на зловредни мрежови действия от приложенията, разположени по работните станции и сървърите в инфраструктурата на организацията. Трябва да има възможност за обновяване на тези правила използвайки актуална информация събрана от вендора за най-новите заплахи.	Предложеното решение предоставя предварително зададени правила за разпознаване на зловредни мрежови действия от приложенията, разположени по работните станции и сървърите в инфраструктурата на организацията. Има възможност за обновяване на тези правила, използвайки актуална информация, събрана от вендора за най-новите заплахи. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.131	Решението трябва да може да анализира мрежови трафик от организацията към Интернет и да засича изпълнението на нежелани приложения или callback комуникации с хакерски командни центрове, като по тази начин да могат да се блокират опити за изнасяне на информация извън организацията по мрежата, като или да се блокира мрежовата сесия ако се работи в inline режим или като вгражда „reset" пакети в комуникацията ако се работи в „out-of-band" режим.	Решението може да анализира мрежови трафик от организацията към Интернет и да засича изпълнението на нежелани приложения или callback комуникации с хакерски командни центрове, като по тази начин могат да се блокират опити за изнасяне на информация извън организацията по мрежата, като или се блокира мрежовата сесия, ако се работи в inline режим или като вгражда „reset" пакети в комуникацията, ако се работи в „out-of-band" режим. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.132	Решението да може да функционира като ICAP сървър, като да може да получава файлове за анализ чрез ICAP протокола.	Решението може да функционира като ICAP сървър, като може да получава файлове за анализ чрез ICAP протокола. Източник: NX SERIES USER GUIDE RELEASE 8.3 Страници: 169
REQ.133	Решението трябва да може да засича ранните фази на уеб-базираните атаки, например първоначално стартиране на exploit, сваляне на	Решението може да засича ранните фази на уеб-базираните атаки, например първоначално [redacted] стартиране на exploit, сваляне на зловреден [redacted]

[redacted]

	зловреден бинарен код, callback функции и комуникации с хакерски командни центрове, за да може да идентифицира уязвимости в системите и приложенията на организацията, за да може да засича заразени системи и за да може да блокира неоторизирани комуникации навън от средата, по няколко мрежови протокола.	бинарен код, callback функции и комуникации с хакерски командни центрове, като по този начин идентифицира уязвимости в системите и приложенията на организацията, засича заразени системи и може да блокира неоторизирани комуникации навън от средата, по няколко мрежови протокола. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.134.	Предложеното решение трябва да може да инспектира и да открива зловредни обекти, зловредни URL мрежови адреси и зловредни действия в поне следните мрежови протоколи: HTTP, HTTPS, FTP, SMB.	Предложеното решение може да инспектира и да открива зловредни обекти, зловредни URL мрежови адреси и зловредни действия в следните мрежови протоколи: HTTP, HTTPS, FTP, SMB. Източник: NX SERIES SMARTVISION FEATURE GUIDE RELEASE 8.3 Страници: 16
REQ.135.	Предложеното решение трябва да може да засича движение на атаките „настрани" в организацията (lateral spread) като анализира SMB, WinRM и MS-SQL трафик и да може да засича и алармира за дейности след успешен exploit на уязвимости от атакуващите, от вътрешна работна станция до вътрешен трафик (трафик тип изток-запад), като например вътрешно разузнаване, ескалиране на права за достъп на акаунти, извличане на потребителски имена и пароли, движение „настрани" на зловреден код, изпълнение на дистанционни команди, извличане на данни.	Предложеното решение може да засича движение на атаките „настрани" в организацията (lateral spread) като анализира SMB, WinRM и MS-SQL трафик и може да засича и алармира за дейности след успешен exploit на уязвимости от атакуващите, от вътрешна работна станция до вътрешен трафик (трафик тип изток-запад), като например вътрешно разузнаване, ескалиране на права за достъп на акаунти, извличане на потребителски имена и пароли, движение „настрани" на зловреден код, изпълнение на дистанционни команди, извличане на данни.

		Източник: NX SERIES SMARTVISION FEATURE GUIDE RELEASE 8.3 Страници: 17
REQ.136	Предложеното решение трябва да е под формата на специализирано хардуерно устройство и вендора трябва да предостави пълни лицензи за софтуера, който ще се използва от устройството за анализиране на зловреден код, както и необходимите лицензи за операционните системи и приложенията, използвани от виртуалната среда за анализ на кода.	Предложеното решение е под формата на специализирано хардуерно устройство и вендорът предоставя пълни лицензи за софтуера, който ще се използва от устройството за анализиране на зловреден код, както и необходимите лицензи за операционните системи и приложенията, използвани от виртуалната среда за анализ на кода. Източник: NX SERIES USER GUIDE RELEASE 8.3 Страници: 108
REQ.137	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението трябва да използва собствен, специално изграден хипервайзор.	Решението не използва комерсиален хипервайзор, който може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението използва собствен, специално изграден хипервайзор. https://www.fireeye.com/content/dam/fireeye-www/company/events/infosec/france-tech-track-summit.pdf Страница 22
REQ.138	Решението трябва да позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите трябва да могат да променят поне следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, използваният Outlook акаунт, езика на машината, времевата зона на машината.	Решението позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите могат да променят поне следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, използвания Outlook акаунт, езика на машината, времевата зона на машината. Източник: NX SERIES USER GUIDE RELEASE 8.3

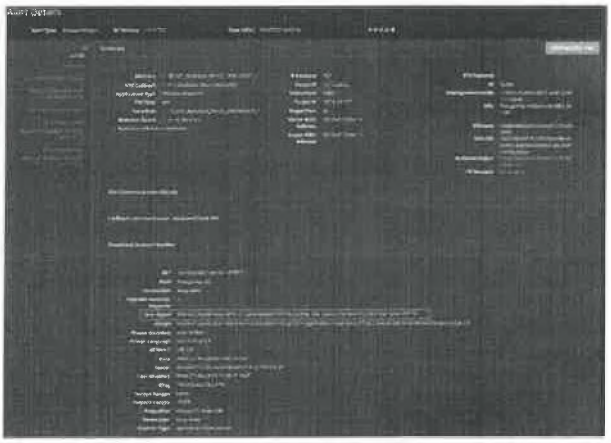
<table>
<tr>
<td></td>
<td></td>
<td>Страници: 116

4. Enter one or more of the following configuration settings:
<table>
<tr><th>Parameter Group</th><th>Fields</th><th>Description</th><th>Response</th></tr>
<tr><td>User Name</td><td>—</td><td>Name of user</td><td>—</td></tr>
<tr><td>Domain Name</td><td>—</td><td>Name of domain</td><td>—</td></tr>
<tr><td>Host Name</td><td>—</td><td>Name of host</td><td>—</td></tr>
<tr><td>Computer Name</td><td>—</td><td>Name of computer</td><td>—</td></tr>
<tr><td>Home Directory</td><td>Home Drive</td><td>Name of a home drive</td><td>—</td></tr>
<tr><td>Windows Recent Files</td><td>File Path</td><td>List of file path names</td><td>Enter a file path name. For example, c:\windows\sample.txt.</td></tr>
<tr><td>Office Recent Files</td><td>Office Recent File Path</td><td>Name of file path</td><td>Enter a file path name. For example, c:\office\recent. txt.</td></tr>
<tr><td>Browser History</td><td>Browser History URL</td><td>List of URLs</td><td>Enter a URL. For example, http://www.google.com.</td></tr>
<tr><td>Honey Credentials</td><td>Type</td><td>System or Browser</td><td>Enter a honey credential that includes type (system or browser), user name, and password. For example, browser:john.smith: honey_password123.</td></tr>
<tr><td></td><td>User Name</td><td>Name of user</td><td>—</td></tr>
<tr><td></td><td>Password</td><td>Password for authenticating honey credential</td><td>—</td></tr>
<tr><td>Honey Files</td><td>Honey File</td><td>List of honey file path names</td><td>—</td></tr>
</table>
</td>
</tr>
<tr>
<td>REQ.139.</td>
<td>Решението трябва да предоставя среда за динамичен анализ, която да се състои от предварително създадени виртуални машини, които да са изцяло предоставени и поддържани от вендора на решението, за да се избегне сложността произтичаща от инсталирането на приложения и поддръжката на виртуални машини от страна на организацията.</td>
<td>Решението предоставя среда за динамичен анализ, която се състои от предварително създадени виртуални машини, които са изцяло предоставени и поддържани от вендора на решението, по този начин се избягва сложността, произтичаща от инсталирането на приложения и поддръжката на виртуални машини от страна на организацията.

https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf</td>
</tr>
<tr>
<td>REQ.140.</td>
<td>Решението трябва да може да идентифицира атаки, без да внася забавяне в мрежовия трафик на организацията, като анализа трябва</td>
<td>Решението може да идентифицира атаки, без да внася забавяне в мрежовия трафик на организацията, като анализът се извършва</td>
</tr>
</table>

	да се извършва локално, на мрежовото ниво, където е разположено устройството.	локално, на мрежовото ниво, където е разположено устройството. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.141	Решението трябва да има механизъм за класифициране и поставяне на етикети на бинарен код на машинно ниво, които се отнася за EXE, DLL и SYS файлове.	Решението има механизъм за класифициране и поставяне на етикети на бинарен код на машинно ниво, които се отнася за EXE, DLL и SYS файлове. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.142	Предложеното решение трябва да дава възможно най-малко грешни показания и да вдига възможно най-малко грешни аларми при засичането на файлове, които наподобяват зловреден код: да алармира за поведение, което опитва да избегне засичане от системите за сигурност, инсталиране на нежелани програми, промяна на системните настройки, което влошава производителността на системите, наличие на потенциално нежелани програми (PUP) и на потенциално нежелани приложения (PUA), adware процеси и използване на инструменти, които често се използват от атакуващи хакери.	Предложеното решение дава възможно най-малко грешни показания и вдига възможно най-малко грешни аларми при засичането на файлове, които наподобяват зловреден код: алармира за поведение, което опитва да избегне засичане от системите за сигурност, инсталиране на нежелани програми, промяна на системните настройки, което влошава производителността на системите, наличие на потенциално нежелани програми (PUP) и на потенциално нежелани приложения (PUA), adware процеси и използване на инструменти, които често се използват от атакуващи хакери. Източник: NX SERIES USER GUIDE RELEASE 8.3 Страници: 160
REQ.143	Решението трябва да може да разпознава заплахи чрез извършване на локален анализ, без да се изпращат файлове, проби от кода или изпълним код извън организацията или към облачно-базирани системи за анализ.	Решението може да разпознава заплахи чрез извършване на локален анализ, без да се изпращат файлове, проби от кода или изпълним код извън организацията или към облачно-базирани системи за анализ.

		https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.144.	Трябва да има възможност за комплексно разследване за целия цикъл на атаките, включително върху всяка от следните фази, за които да има отделни аларми: • Първоначално разпознаване на мрежата (Картографиране на мрежата, преброяване на хостовете, преброяване на услугите, издирване на потребителски акаунти); • Изпълнение (използване на командата „AT" за насрочване на изпълнение на процеси, „pass-the-hash" дистанционно изпълнение на код (RCE), използване на инструментариума за управление на Windows средите (WMI), дистанционно създаване на процеси); • Изпълнение на Web Shell; • Сваляне на зловреден код (malware); • Извличане на информация чрез свързвания с хакерски команден сървър; • Разпространяване на зловредния код (трансфер на зловреден код чрез SMB и SMB 2 протоколи) • Ескалиране на привилегии (преброяване на групите с високо ниво на достъп, преброяване на дистанционно споделените ресурси - remote shares) • Извличане на данни за вписване в системите (трансфер на пароли чрез SMB протокол, извличане чрез Mimikatz, извличане на NTLM хешове) • Дистанционно изпълнение на процеси.	Има възможност за комплексно разследване за целия цикъл на атаките, включително върху всяка от следните фази, за които има отделни аларми: • Първоначално разпознаване на мрежата (Картографиране на мрежата, преброяване на хостовете, преброяване на услугите, издирване на потребителски акаунти); • Изпълнение (използване на командата „AT" за насрочване на изпълнение на процеси, „pass-the-hash" дистанционно изпълнение на код (RCE), използване на инструментариума за управление на Windows средите (WMI), дистанционно създаване на процеси); • Изпълнение на Web Shell; • Сваляне на зловреден код (malware); • Извличане на информация чрез свързвания с хакерски команден сървър; • Разпространяване на зловредния код (трансфер на зловреден код чрез SMB и SMB 2 протоколи) • Ескалиране на привилегии (преброяване на групите с високо ниво на достъп, преброяване на дистанционно споделените ресурси - remote shares) • Извличане на данни за вписване в системите (трансфер на пароли чрез SMB протокол, извличане чрез Mimikatz, извличане на NTLM хешове) • Дистанционно изпълнение на процеси.

		Източник: NX SERIES SMARTVISION FEATURE GUIDE RELEASE 8.3 Страници: 225 https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.145.	Решението трябва да може да идентифицира уеб-базирани уязвимости, чрез извършване на анализ на съмнително уеб съдържание във виртуалните машини за анализ, използвайки същия тип браузър, както реалния потребител достъпил уеб съдържанието.	Решението може да идентифицира уеб-базирани уязвимости, чрез извършване на анализ на съмнително уеб съдържание във виртуалните машини за анализ, използвайки същия тип браузър, както реалния потребител, достъпил уеб съдържанието. 
REQ.146.	Решението трябва да може да засича атаки към сървърите като извлича и анализира статични и динамични уеб-базирани файлове (PHP, WAR, JSP, ASP, ASPX), които са качени на уеб сървърите чрез HTTP POST или FTP.	Решението може да засича атаки към сървърите като извлича и анализира статични и динамични уеб-базирани файлове (PHP, WAR, JSP, ASP, ASPX), които са качени на уеб сървърите чрез HTTP POST или FTP. Източник: NX SERIES RELEASE NOTES RELEASE 8.3 Страници: 11
REQ.147.	Решението трябва да предоставя детайлна информация за аларми, произлизащи от извлечените метаданни от транспортния и от	Решението предоставя детайлна информация за аларми, произлизащи от извлечените метаданни от транспортния и от приложния слой на мрежата,

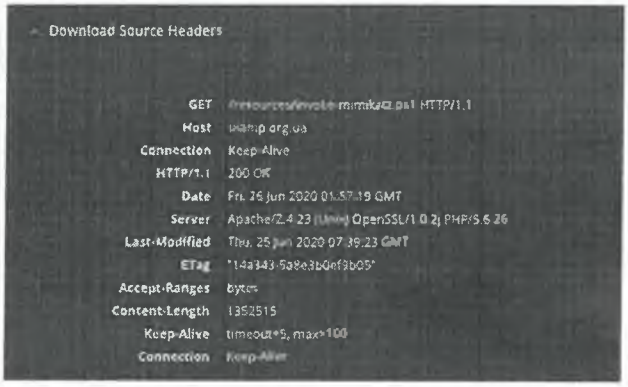
	приложния слой на мрежата, за поне следните протоколи: FTP, HTTP, IMAP, IRC, POP3, RDP, RTSP, SIP, SMB, SMTP, SSH, TLS; Решението трябва да може да визуализира метаданните в интерактивна, графична форма, както и да позволява извличането им за интегриране с трети SIEM решения.	за следните протоколи: FTP, HTTP, IMAP, IRC, POP3, RDP, RTSP, SIP, SMB, SMTP, SSH, TLS; Решението може да визуализира метаданните в интерактивна, графична форма, както и да позволява извличането им за интегриране с трети SIEM решения. Източник: NX SERIES SMARTVISION FEATURE GUIDE RELEASE 8.3 Страници: 144, 227
REQ.148.	Решението трябва да може да инспектира HTTPS трафик, като да се поддържат SSL / TLS протоколи, включително да се поддържат функции като JA3 fingerprinting, използване на „бели списъци" и URL категоризация.	Решението може да инспектира HTTPS трафик, като да се поддържат SSL / TLS протоколи, включително се поддържат функции като JA3 fingerprinting, използване на „бели списъци" и URL категоризация. Източник: NX SERIES RELEASE NOTES RELEASE 8.3
REQ.149.	Решението трябва да може да анализира поне следните файлови типове: msi, exe, dll, pdf, doc, chm, avi, jar, docx, xls, xlsx, gif, jpeg, png, tiff, swf, swf embedded in swf, scr, mov, qt, mp4, jpg, mp3, asf, ico, htm, hta, url, rm, com, vcf, ppt, rtf, chm, hlp и други.	Решението може да анализира следните файлови типове: msi, exe, dll, pdf, doc, chm, avi, jar, docx, xls, xlsx, gif, jpeg, png, tiff, swf, swf embedded in swf, scr, mov, qt, mp4, jpg, mp3, asf, ico, htm, hta, url, rm, com, vcf, ppt, rtf, chm, hlp и други. **WIN10 x64**

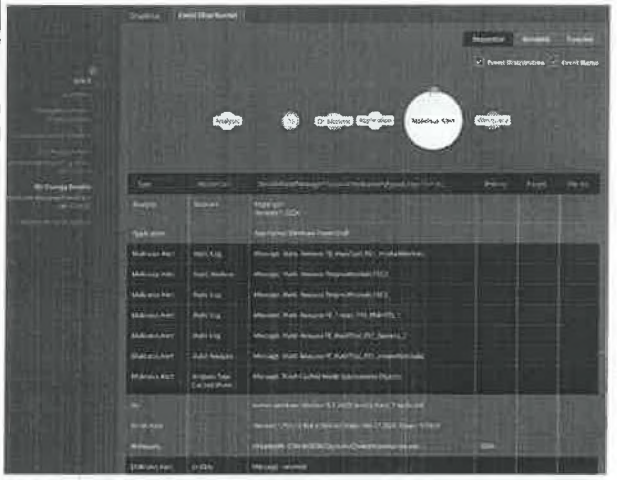
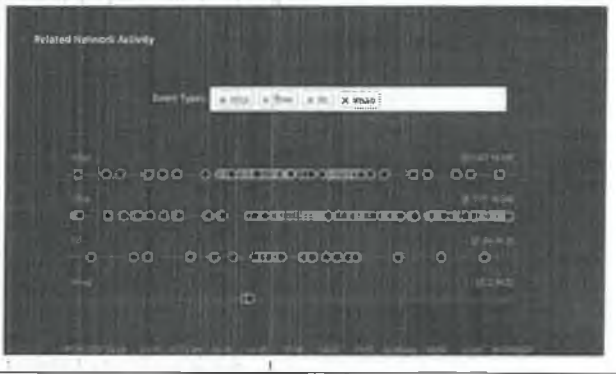
WIN XP

		OSX
REQ.150.	Решението трябва да предоставя „предварителен изглед" на засечените съмнителни URL адреси, като да може да предоставя на анализаторите screenshot-и от URL адресите.	Решението предоставя „предварителен изглед" на засечените съмнителни URL адреси, като може да предоставя на анализаторите screenshot-и от URL адресите. Източник: NX SERIES RELEASE NOTES RELEASE 8.3 Страници: 12
REQ.151.	Решението трябва да може да извършва динамичен анализ за зловреден код, да може да се обновява и да може да му се предоставя нова информация за заплахи, дори в offline режим, без да има връзка с Интернет.	Решението може да извършва динамичен анализ за зловреден код, може да се обновява и може да му се предоставя нова информация за заплахи, дори в offline режим, без да има връзка с Интернет. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.152.	Решението трябва да може да предоставя контекстуална информация към вдигнатите аларми, като например източник, степен на опасност, потенциални рискове, варианти за справяне с проблема и т.н., за засечените атаки от дадена рискова група.	Решението може да предоставя контекстуална информация към вдигнатите аларми, като например източник, степен на опасност, потенциални рискове, варианти за справяне с проблема и т.н., за засечените атаки от дадена рискова група.

		https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.153.	Решението трябва да разполага с голям набор от виртуални машини за sandbox анализ, с предварително инсталирани операционни системи и софтуер, бивайки Windows OS (включително XP, 7, 10), Mac OSX и Linux Cent OS, с различни версии на Service Pack, 32 и 64 битови, за да може да извършва точен анализ на поведението на процесите според различните уязвимости на средите.	Решението разполага с голям набор от виртуални машини за sandbox анализ, с предварително инсталирани операционни системи и софтуер, бивайки Windows OS (включително XP, 7, 10), Mac OSX и Linux Cent OS, с различни версии на Service Pack, 32 и 64 битови, като по този начин извършва точен анализ на поведението на процесите според различните уязвимости на средите.
REQ.154.	Решението трябва да предоставя множество приложения с различни версии за тестове, разположени на виртуалните машини за анализ на зловредни файлове. Приложенията и версиите трябва да бъдат минимум следните: Microsoft Office 2003, 2007, 2010, 2013; Adobe Reader 7, 8, 9, 10, 11; Internet explorer 6, 7, 8, 9, 10, 11.	Решението предоставя множество приложения с различни версии за тестове, разположени на виртуалните машини за анализ на зловредни файлове. Приложенията и версиите са следните: Microsoft Office 2003, 2007, 2010, 2013; Adobe Reader 7, 8, 9, 10, 11; Internet explorer 6, 7, 8, 9, 10, 11. Източник: NX Platform.doc
REQ.155.	Решението трябва да може да анализира един и същ файл на различни видове и версии на операционни системи и приложения, както и на различни версии на Internet Explorer, за да се открие потенциално зловредно поведение използващо конкретни уязвимости.	Решението може да анализира един и същ файл на различни видове и версии на операционни системи и приложения, както и на различни версии на Internet Explorer, за да се открие потенциално зловредно поведение, използващо конкретни уязвимости.

		https://www.fireeye.com/content/dam/fireeye-www/company/events/infosec/france-tech-track-summit.pdf Страница 22
REQ.156.	Решението трябва да може да алармира за зловредни процеси, които не са били засечени в първоначалните 24 часа, а на по-късен етап е установено, че са зловредни.	Решението може да алармира за зловредни процеси, които не са били засечени в първоначалните 24 часа, а на по-късен етап е установено, че са зловредни. Източник: NX SERIES USER GUIDE RELEASE 8.3 Страници: 368
REQ.157.	След извършване на анализ, решението трябва да може да предоставя пълен отчет за него, който да съдържа минимално следната информация: • Тип на анализираните файлове; • Име на пробата; • Контролните суми на анализираните файлове (MD5, SHA1 / 256/512); • Класификация според това към кое семейство се причислява засечения зловреден код; • Тип на използваната уязвимост за пробив; • URL адреси, които са използвани за атаката, както и предоставяне на информация за преглед на съдържанието на URL адресите чрез изображения (screenshots); • Данни за идентифициране на заразените системи (IP, MAC); • Графично изобразяване на поведението на анализирания зловреден код;	След извършване на анализ, решението може да предоставя пълен отчет за него, който съдържа следната информация: • Тип на анализираните файлове; • Име на пробата; • Контролните суми на анализираните файлове (MD5, SHA1 / 256/512); • Класификация според това, към кое семейство се причислява засечения зловреден код; • Тип на използваната уязвимост за пробив; • URL адреси, които са използвани за атаката, както и предоставяне на информация за преглед на съдържанието на URL адресите чрез изображения (screenshots); • Данни за идентифициране на заразените системи (IP, MAC); • Графично изобразяване на поведението на анализирания зловреден код; • Извършени промени по операционните системи;

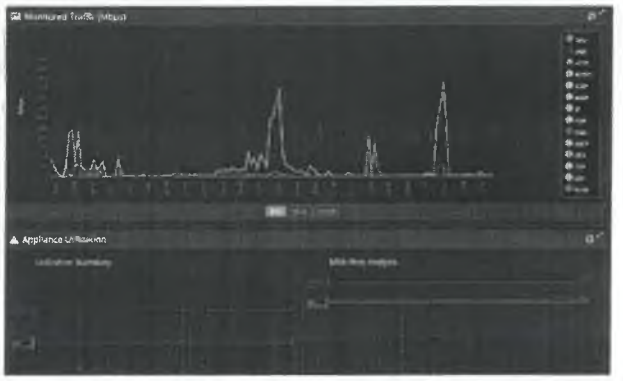
	• Извършени промени по операционните системи; • Извършени промени по инсталираните приложения на виртуалните машини за анализ; • Извършени промени по файловата система; • Извършени промени по регистрите на Windows операционните системи; • Качените DLL библиотеки; • Извиканите Windows API функции, в хронологичен ред; • Информация за създадените / модифицираните / спрените процеси; • Детайлно изобразяване на поведението на процесите на мрежово ниво в графичен формат (изпълнени мрежови свързвания и използваните транспортни мрежови протоколи, използвани портове, DNS заявки и отговори, http пакети); • Информация за IP адресите, с които е комуникирано;	• Извършени промени по инсталираните приложения на виртуалните машини за анализ; • Извършени промени по файловата система; • Извършени промени по регистрите на Windows операционните системи; • Качените DLL библиотеки; • Извиканите Windows API функции, в хронологичен ред; • Информация за създадените / модифицираните / спрените процеси; • Детайлно изобразяване на поведението на процесите на мрежово ниво в графичен формат (изпълнени мрежови свързвания и използваните транспортни мрежови протоколи, използвани портове, DNS заявки и отговори, http пакети); • Информация за IP адресите, с които е комуникирано; 

		   
REQ.158.	Решението трябва да може да съхранява данните от изпълнението на зловреден код и прилежащите артефакти, като например PCAP файл с данни от засечените заплахи, за да може	Решението може да съхранява данните от изпълнението на зловреден код и прилежащите артефакти, като например PCAP файл с данни от засечените заплахи, за да може информацията да се анализира допълнително и след извършения sandbox анализ.

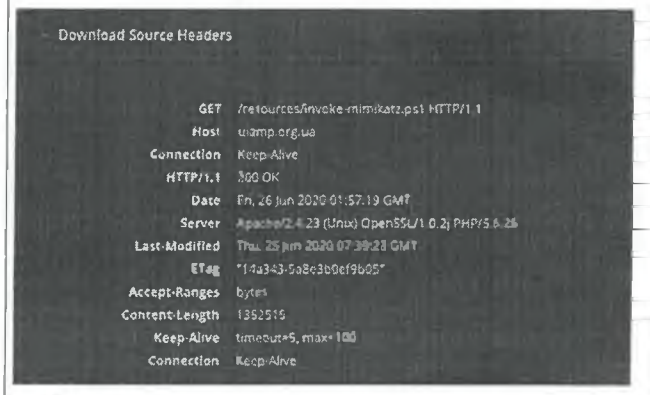
	информацията да се анализира допълнително и след извършения sandbox анализ.	
REQ.159.	Решението трябва да може да се поставя в следните режими на работа: SPAN, TAP, inline или HW bypass.	Решението може да се поставя в следните режими на работа: SPAN, TAP, inline или HW bypass. Източник: NX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 65-85
REQ.160.	Решението трябва да позволява използването на YARA правила.	Решението позволява използването на YARA правила. Източник: NX SERIES USER GUIDE RELEASE 8.3 Страници: 125
REQ.161.	Решението трябва да може да анализира мрежови трафик независимо от използваните VLAN и портове, без да изисква предварително задаване на параметри, включително да се поддържат протоколи Encapsulated remote SPAN, Virtual Extensible LAN и Internet Content Adaptation Protocol.	Решението може да анализира мрежови трафик независимо от използваните VLAN и портове, без да изисква предварително задаване на параметри, включително се поддържат протоколи Encapsulated remote SPAN, Virtual Extensible LAN и Internet Content Adaptation Protocol. Източник: NX SERIES USER GUIDE RELEASE 8.3 Страници: 70, 382
REQ.162.	Решението трябва да разполага с команден и с графичен интерфейс (достъпен през стандартен уеб-браузър) за централизирано управление, без да се изисква инсталиране на допълнителен софтуер.	Решението разполага с команден и с графичен интерфейс (достъпен през стандартен уеб-браузър) за централизирано управление, не се изисква инсталиране на допълнителен софтуер. Източник: NX SERIES USER GUIDE RELEASE 8.3 Страници: 20-21

REQ.163.	Решението трябва да поддържа ролево-базиран достъп до конзолата за управление. Да могат да се задават различни профили и права (администратор, оператор, одитор и т.н.), като да се задават кои отчети, аларми и информация могат да виждат в конзолата за управление.	Решението поддържа ролево-базиран достъп до конзолата за управление. Могат да се задават различни профили и права (администратор, оператор, одитор и т.н.), като се задават кои отчети, аларми и информация могат да виждат в конзолата за управление. Източник: SYSTEM SECURITY SYSTEM SECURITY GUIDE RELEASE 2019.4 Страници: 373
REQ.164.	Решението трябва да може да анализира и засича атаки, които протичат на няколко нива и фази, а да не предоставя само sandbox технология за анализ на отделни файлове в изолация.	Решението може да анализира и засича атаки, които протичат на няколко нива и фази, а не предоставя само sandbox технология за анализ на отделни файлове в изолация. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.165.	Решението трябва да борави с различни версии на Microsoft Office във виртуалните машини за анализ, като да може да анализира Microsoft Office документи с вграден зловреден код или макроси за пароли, анализ на зловреден трафик от тях, както и да се засичат системни грешки свързани с документите.	Решението борави с различни версии на Microsoft Office във виртуалните машини за анализ, като може да анализира Microsoft Office документи с вграден зловреден код или макроси за пароли, анализ на зловреден трафик от тях, както и засича системни грешки, свързани с документите. https://www.fireeye.com/content/dam/fireeye-www/company/events/infosec/france-tech-track-summit.pdf Страница 22
REQ.166.	Решението трябва да може да засича и класифицира следните категории атаки: • Ransomware криптиращи атаки; • Следи от meterpreter команди; • Кражба на файлове;	Решението може да засича и класифицира следните категории атаки: • Ransomware криптиращи атаки; • Следи от meterpreter команди; • Кражба на файлове;

	• Инфектиране на файлове; • Опити за силово разбиване на пароли; • Изпълнение на команди; • Използване на уязвимости за пробив (exploit); • Атаки с цел разузнаване;	• Инфектиране на файлове; • Опити за силово разбиване на пароли; • Изпълнение на команди; • Използване на уязвимости за пробив (exploit); • Атаки с цел разузнаване; Източник: Guest Images 14.1110 Източник: NX_IPS_8.3.0_en.pdf Страници: 20-21
REQ.167.	Решението трябва да може да анализира причините за принудително спиране на дадено приложение.	Решението може да анализира причините за принудително спиране на дадено приложение. Източник: Guest Images 14.1110 Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0101
REQ.168.	Решението трябва да може да получава информация за нови киберзаплахи от глобална система за информация на производителя.	Решението може да получава информация за нови киберзаплахи от глобална система за информация на производителя. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.169.	Решението трябва да може да получава системни обновления и обновления за виртуалниите машини за анализ, директно от уеб-базирания интерфейс за централизирано управление на решението.	Решението може да получава системни обновления и обновления за виртуалниите машини за анализ, директно от уеб-базирания интерфейс за централизирано управление на решението.

REQ.170.	Решението трябва да предоставя информация за системните си показатели в графичния интерфейс за управление.	Решението предоставя информация за системните си показатели в графичния интерфейс за управление. 
REQ.171.	Решението трябва да позволява използването на прокси сървър с оторизация за сваляне на обновления.	Решението позволява използването на прокси сървър с оторизация за сваляне на обновления. Източник: NX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 110
REQ.172.	Решението трябва да може с точност да идентифицира и обособи филтриран и блокиран мрежови трафик през уеб прокси.	Решението може с точност да идентифицира и обособи филтриран и блокиран мрежови трафик през уеб прокси. Източник: NX SERIES USER GUIDE RELEASE 8.3 Страници: 392
REQ.173.	Решението трябва да позволява филтриране на мрежови трафик, да се определя дали да се анализира или блокира трафика, като се използват „бели списъци". Трябва да може да се филтрира на базата на: Generic Routing	Решението позволява филтриране на мрежови трафик, може да определя, дали да се анализира или блокира трафика, като се използват „бели списъци". Може да се филтрира на базата на: Generic Routing Encapsulation, използвани портове

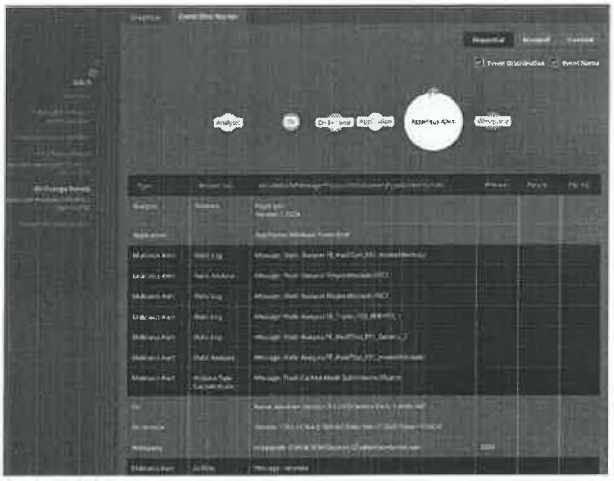
	Encapsulation, използвани портове за комуникация и филтриране на конкретни мрежи (по зададени IP адреси или подмрежи).	за комуникация и филтриране на конкретни мрежи (по зададени IP адреси или подмрежи). Източник: NX SERIES USER GUIDE RELEASE 8.3 Страници: 82
REQ.174.	Решението трябва да поддържа LDAP, TACACS + или RADIUS методи за вписване на потребителите.	Решението поддържа LDAP, TACACS + или RADIUS методи за вписване на потребителите. Източник: SYSTEM SECURITY SYSTEM SECURITY GUIDE RELEASE 2019.4 Страници: 57-67
REQ.175.	Решението трябва да може да използва XFF хедъри за идентифициране на коя машина генерира аларми, когато се намира зад прокси сървър.	Решението може да използва XFF хедъри за идентифициране на коя машина генерира аларми, когато се намира зад прокси сървър. Източник: NX SERIES USER GUIDE RELEASE 8.3 Страници: 389
REQ.176.	Решението не трябва да позволява мрежова комуникация от виртуалните машини за анализ към Интернет и от анализирания зловреден код към хакерски команден център или към URL адрес.	Решението не позволява мрежова комуникация от виртуалните машини за анализ към Интернет и от анализирания зловреден код към хакерски команден център или към URL адрес. Източник: NX SERIES USER GUIDE RELEASE 8.3 Страници: 56
REQ.177.	По време на извършван анализ, ако зловредния код изпрати заявка за сваляне на допълнителни файлове (двоичен код), решението трябва да може да предостави на виртуалната машина заместващ доброкачествен файл, за да се продължи изпълнението и анализа.	По време на извършван анализ, ако зловредният код изпрати заявка за сваляне на допълнителни файлове (двоичен код), решението може да предостави на виртуалната машина заместващ доброкачествен файл, за да се продължи изпълнението и анализа. Източник: NX SERIES USER GUIDE RELEASE 8.3 Страници: 61

REQ.178.	Решението трябва да може да предоставя следната информация: • Доклад с промените по системите; • Копие на зловредния двоичен код; • Мета данни от зловредния код; • Уловен мрежови трафик (PCAP файл) от виртуалните машини за анализ; • Пълно описание на достъпените URL адреси от зловредния код с идентифициране на локациите им.	Решението може да предоставя следната информация: • Доклад с промените по системите; • Копие на зловредния двоичен код; • Мета данни от зловредния код; • Уловен мрежови трафик (PCAP файл) от виртуалните машини за анализ; • Пълно описание на достъпените URL адреси от зловредния код с идентифициране на локациите им. 

[redacted]

[redacted]

[redacted]

		  
REQ.179.	Решението трябва да може да предоставя извличането на отчети и аларми в PDF формат.	Решението може да предоставя извличането на отчети и аларми в PDF формат. Източник: NX SERIES USER GUIDE RELEASE 8.3 Страници: 25
REQ.180.	Решението трябва да може да определи степента на заплаха на даден инцидент от вдигнатите аларми за него.	Решението може да определи степента на заплаха на даден инцидент от вдигнатите аларми за него. Източник: NX SERIES USER GUIDE RELEASE 8.3 Страници: 64

REQ.181.	Решението трябва да може да вдига различни аларми за всяка фаза от жизнения цикъл на засечените атаки.	Решението може да вдига различни аларми за всяка фаза от жизнения цикъл на засечените атаки. Източник: NX SERIES USER GUIDE RELEASE 8.3 Страници: 63-64
REQ.182.	Решението трябва да може да засича опити за използване на функциите за приспиване (sleep) на операционните системи от зловредния код и да може да забързва времето на виртуалните машини за анализ, за да принуди изпълнението на зловредния код.	Решението може да засича опити за използване на функциите за приспиване (sleep) на операционните системи от зловредния код и може да забързва времето на виртуалните машини за анализ, за да принуди изпълнението на зловредния код.
REQ.183.	Решението трябва да може да симулира потребителски действия, за да изпълни зловреден код изискващ подобни действия, като например щракане с мишката или конфигуриране на конкретни данни.	Решението може да симулира потребителски действия, за да изпълни зловреден код, изискващ подобни действия, като например щракане с мишката или конфигуриране на конкретни данни. https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/pf/file/fireeye-hot-knives-through-butter.pdf
REQ.184.	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques), например използване на ping команди, проверка на домейн, проверка на отметки в наличните браузъри.	Решението може да се справя с техники за избягване от засичане (evasion techniques), например използване на ping команди, проверка на домейн, проверка на отметки в наличните браузъри. Източник: NX SERIES USER GUIDE RELEASE 8.3

		Страници: 116
REQ.185.	Решението трябва да може да изпраща известия за собственото си здраве и процеси, на базата на SMTP, до предварително зададени локации.	Решението може да изпраща известия за собственото си здраве и процеси, на базата на SMTP, до предварително зададени локации. Източник: SYSTEM SECURITY SYSTEM SECURITY GUIDE RELEASE 2019.4 Страници: 155
REQ.186.	Решението трябва да може да се интегрира (за обмен на информация) с подсистемата за улавяне на мрежови пакети, разследвания и централизиран анализ и визуализация, с подсистемата за засичане, разследвания и защита от познати и непознати заплахи на ниво крайна точка и с подсистемата за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения.	Решението може да се интегрира (за обмен на информация) с подсистемата за улавяне на мрежови пакети, разследвания и централизиран анализ и визуализация, с подсистемата за засичане, разследвания и защита от познати и непознати заплахи на ниво крайна точка и с подсистемата за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения. Източник: CENTRAL MANAGEMENT ADMINISTRATION GUIDE RELEASE 8.7 Страници: 433, 440
REQ.187.	Решението трябва да предоставя опция да получава и изпраща обекти за анализ, когато бъде достигнат зададен лимит на капацитета на обработваните обекти от решението, към предварително зададен локално-разположен клъстър или към специализирани хардуерни устройства за балансиране на производителността.	Решението предоставя опция да получава и изпраща обекти за анализ, когато бъде достигнат зададен лимит на капацитета на обработваните обекти от решението, към предварително зададен локално-разположен клъстър или към специализирани хардуерни устройства за балансиране на производителността. Източник: NX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 87

	Хардуерни изисквания – 2 броя	**Предложение: 2 броя хардуерни устройства (High-Availability) с вграден софтуер FireEye HW-NX 5500 с включена 5-годишна поддръжка и 2 допълнителни разширителни модула x 1G-10G BASE-LX/LR FIBER**
REQ.188.	Производителност мрежова защита, мрежови трафик: минимално 2.4 Gbps	Устройството разполага с производителност за мрежова защита на мрежови трафик: 2.5 Gbps https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.189.	Производителност на вградена IPS функционалност, мрежови трафик: минимално 2.4 Gbps	Устройството разполага с производителност на вградена IPS функционалност за мрежова защита на мрежови трафик: 2.5 Gbps https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.190.	Минимален брой поддържани едновременни сесии за IPS: 1M	Устройството поддържа 1M едновременни сесии за IPS https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.191.	Минимален брой поддържани нови сесии в секунда за IPS: 20K/Sec	Устройството поддържа 20K/Sec нови сесии в секунда за IPS https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.192.	Устройството да е с максимална големина 2RU	Устройството е с големина 2RU https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf

[redacted] [redacted] [redacted] [redacted]

REQ.193.	Устройството да разполага с поне 4TB за съхранение на данни	Устройството разполага с 2 x 4TB за съхранение на данни https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.194.	Устройството да разполага минимално със следните портове за наблюдение на мрежата: 8x 10GigE SFP+; 4x 1GigE Bypass и 2 допълнителни разширителни модула x 1G-10G BASE-LX/LR FIBER	Устройството разполага със следните портове за наблюдение на мрежата: 8x 10GigE SFP+; 4x 1GigE Bypass и 2 допълнителни разширителни модула x 1G-10G BASE-LX/LR FIBER https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.195.	Устройството да поддържа следните режими на работа на портовете за наблюдение на мрежата: In-line Monitor, Fail-Open, Fail- Close (HW Bypass) или TAP/SPAN	Устройството поддържа следните режими на работа на портовете за наблюдение на мрежата: in-line Monitor, Fail-Open, Fail- Close (HW Bypass) или TAP/SPAN https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.196.	Допълнителни портове: 2x 1GigE портове за управление, сериен порт, 4x Type A USB, IPMI, VGA	Устройството разполага със следните допълнителни портове: 2x 1GigE портове за управление, сериен порт, 4x Type A USB, IPMI, VGA https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.197.	Резервирано захранване – 1+1	Устройството разполага с резервирано захранване – 1+1

		https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.198.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.	Устройството работи в изолиран режим, без Интернет свързаност. Устройството не изпраща данни към производителя за засечените заплахи в организацията. https://www.fireeye.com/company/legal.html
Гаранция и поддръжка:		**Предлагана гаранция и поддръжка от производителя:**
REQ.199.	Срок на хардуерната гаранция - минимум 5 (пет) години.	Срокът на хардуерната гаранция е 5 (пет) години.
REQ.200.	Срок на техническа поддържка – минимум 5 (пет) години.	Срокът на техническа поддръжка е 5 (пет) години.
REQ.201.	Получаване на нови версии на софтуера - минимум 5 (пет) години.	Новите версии на софтуера ще се получават 5 (пет) години.
REQ.202.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.	Обновяването на дефиниции и сигнатури е 5 (пет) години.

1.4.4. Подсистема за централизирано управление

Изискано от Възложителя		**Предложено от участника**
А.		**Б.**
Общи изисквания		
REQ.203.	Тип решение: 1 брой хардуер с вграден софтуер и 5-годишна поддръжка	Предлаганата подсистема за централизирано управление включва **1 брой хардуерно устройство с вграден софтуер FireEye 7500CM-HW CMS с включена 5-годишна поддръжка**
REQ.204.	Решението трябва да може да извършва корелация на аларми между подсистемата за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво и подсистема за	Решението може да извършва корелация на аларми между подсистемата за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво и подсистемата за динамичен

	динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения, както и подсистемата за засичане, разследвания и защита от познати и непознати заплахи на ниво крайна точка, за да се предостави защита от атаки, които се изпълняват на няколко нива и през няколко вектора. Например: атака чрез зловреден URL адрес, предоставен чрез съдържанието на електронно email съобщение, с прилежащ свален през уеб трафик зловреден файл, който е изпълнен на крайна точка, довело до нейното заразяване.	анализ на зловреден код и защита от кибератаки на електронни email съобщения, както и подсистемата за засичане, разследвания и защита от познати и непознати заплахи на ниво крайна точка, като по тизи начин се предоставя защита от атаки, които се изпълняват на няколко нива и през няколко вектора. Например: атака чрез зловреден URL адрес, предоставен чрез съдържанието на електронно email съобщение, с прилежащ свален през уеб трафик зловреден файл, който е изпълнен на крайна точка, довело до нейното заразяване. Източник: CENTRAL MANAGEMENT ADMINISTRATION GUIDE RELEASE 9.0 Страници: 407
REQ.205.	Решението трябва да може да предоставя и изпълнява обновления на системния софтуер на управляваните от него подсистеми, да може предоставя на подсистемите обновления на информацията за нови заплахи и нови индикатори за компроментиране от глобалната система за информация на производителя или от трети източници.	Решението може да предоставя и изпълнява обновления на системния софтуер на управляваните от него подсистеми, може да предоставя на подсистемите обновления на информацията за нови заплахи и нови индикатори за компроментиране от глобалната система за информация на производителя или от трети източници. Източник: CENTRAL MANAGEMENT ADMINISTRATION GUIDE RELEASE 9.0 Страници: 477
REQ.206.	Решението трябва да поддържа интеграция с подсистемата (лаборатория) за динамичен анализ на зловреден код, за обмен на информация.	Решението поддържа интеграция с подсистемата (лаборатория) за динамичен анализ на зловреден код, за обмен на информация.

		Източник: CENTRAL MANAGEMENT ADMINISTRATION GUIDE RELEASE 9.0 Страници: 322-323
REQ.207.	Решението трябва да може да предоставя детайлни отчети, включително и обединена информация от управляваните подсистеми от решението.	Решението може да предоставя детайлни отчети, включително и обединена информация от управляваните подсистеми от решението. Източник: CENTRAL MANAGEMENT ADMINISTRATION GUIDE RELEASE 9.0 Страници: 361
REQ.208.	Решението трябва да може да управлява генерираните аларми от управляваните подсистеми и да може да изпраща известия, таблици и графики с данните от тях.	Решението може да управлява генерираните аларми от управляваните подсистеми и може да изпраща известия, таблици и графики с данните от тях. Източник: CENTRAL MANAGEMENT ADMINISTRATION GUIDE RELEASE 9.0 Страници: 25
REQ.209.	Решението трябва да предоставя единна конзола, от която да може да се извършва централизирано конфигуриране на управляваните подсистеми, задаване на политики за сигурност, обновяване на информацията за заплахите / индикаторите за компроментиране, обновяване на системния софтуер на подсистемите.	Решението предоставя единна конзола, от която може да се извършва централизирано конфигуриране на управляваните подсистеми, задаване на политики за сигурност, обновяване на информацията за заплахите / индикаторите за компроментиране, обновяване на системния софтуер на подсистемите. Източник: CENTRAL MANAGEMENT ADMINISTRATION GUIDE RELEASE 9.0 Страници: 25
REQ.210.	Решението трябва да позволява обновяване на управляваните подсистеми и информацията за нови заплахи дори в offline режим, без да е необходима свързаност с Интернет.	Решението позволява обновяване на управляваните подсистеми и информацията за нови заплахи дори в offline режим, без да е необходима свързаност с Интернет.

		Източник: CENTRAL MANAGEMENT ADMINISTRATION GUIDE RELEASE 9.0 Страници: 191
REQ.211.	Решението трябва да предоставя интегрирана централизирана администрация, в реално време, използвайки графичен интерфейс, който да предоставя следните функции: • Преглед и филтриране на събития свързани със сигурността; • Идентифициране на заразени устройства; • Централизиране на всички известия и аларми от управляваните подсистеми; • Персонализиране на графичното изобразяване на информацията (персонализиране на dashboards); • Създаване и извличане на отчети в PDF и HTML формати.	Решението предоставя интегрирана централизирана администрация, в реално време, използвайки графичен интерфейс, който има следните функции: • Преглед и филтриране на събития свързани със сигурността; • Идентифициране на заразени устройства; • Централизиране на всички известия и аларми от управляваните подсистеми; • Персонализиране на графичното изобразяване на информацията (персонализиране на dashboards); • Създаване и извличане на отчети в PDF и HTML формати. Източник: CENTRAL MANAGEMENT ADMINISTRATION GUIDE RELEASE 9.0 Страници: 25
REQ.212.	Решението трябва да позволява използването и дистрибутирането на индикатори за компроментиране от трети източници (индикатори, които могат да бъдат URL адреси, IP адреси, домейни и хеш суми на зловредни файлове) към управляваните подсистеми. Индикаторите за компроментиране трябва да могат да се управляват или чрез използването на списъци за всяка категория или чрез	Решението позволява използването и дистрибутирането на индикатори за компроментиране от трети източници (индикатори, които могат да бъдат URL адреси, IP адреси, домейни и хеш суми на зловредни файлове) към управляваните подсистеми. Индикаторите за компроментиране могат да се управляват или чрез използването на списъци за всяка категория или чрез използването на STIX (Structured Threat Information Expression) формат.

	използването на STIX (Structured Threat Information Expression) формат.	Източник: CENTRAL MANAGEMENT ADMINISTRATION GUIDE RELEASE 9.0 Страници: 483
REQ.213.	Решението трябва да поддържа LDAP, TACACS + или RADIUS методи за вписване на потребителите, както и чрез Активна Директория или решения за двуфакторна автентикация.	Решението поддържа LDAP, TACACS + или RADIUS методи за вписване на потребителите, както и чрез Активна Директория или решения за двуфакторна автентикация. Източник: SYSTEM SECURITY SYSTEM SECURITY GUIDE RELEASE 2019.4 Страници: 57-67
REQ.214.	Решението трябва да може да създава, съхранява и предоставя log файлове към трети решения, използвайки Syslog протокол, например за предоставяне на информация на решения от тип SIEM.	Решението да създава, съхранява и предоставя log файлове към трети решения, използвайки Syslog протокол, например за предоставяне на информация на решения от тип SIEM. Източник: CENTRAL MANAGEMENT ADMINISTRATION GUIDE RELEASE 9.0 Страници: 209
Хардуерни изисквания – 1 брой		**Предложение: 1 брой хардуерно устройство с вграден софтуер FireEye 7500CM-HW CMS и с включена 5-годишна поддръжка**
REQ.215.	Устройството да е с максимална големина 2RU	Устройството е с големина 2RU https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/fireeye-cm-series.pdf
REQ.216.	Устройството да разполага с поне 4TB за съхранение на данни	Устройството разполага с 4 x 4TB за съхранение на данни https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/fireeye-cm-series.pdf
REQ.217.	Устройството да разполага минимално със следните портове за свързване с мрежата: 2x 1GigE BaseT	Устройството разполага със следните портове за свързване с мрежата: 2x 1GigE BaseT

		https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/fireeye-cm-series.pdf
REQ.218.	Допълнителни портове: 2x 1GigE BaseT портове за управление, сериен порт, 2x Type A USB, IPMI, VGA	Устройството разполага със следните допълнителни портове: 2x 1GigE BaseT портове за управление, сериен порт, 2x Type A USB, IPMI, VGA https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/fireeye-cm-series.pdf
REQ.219.	Резервирано захранване – 1+1	Устройството разполага с резервирано захранване – 1+1 https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/fireeye-cm-series.pdf
REQ.220.	Устройството да може да управлява другите устройства за защита на крайни точки, за мрежова защита и за email защита, като всички те трябва да бъдат от един производител	Устройството може да управлява другите устройства за защита на крайни точки, за мрежова защита и за email защита, като всички те са от един производител Източник: CENTRAL MANAGEMENT ADMINISTRATION GUIDE RELEASE 9.0 Страници: 322-323
Гаранция и поддръжка:		**Предлагана гаранция и поддръжка от производителя:**
REQ.221.	Срок на хардуерната гаранция - минимум 5 (пет) години.	Срокът на хардуерната гаранция е 5 (пет) години.
REQ.222.	Срок на техническа поддържка – минимум 5 (пет) години.	Срокът на техническа поддръжка е 5 (пет) години.
REQ.223.	Получаване на нови версии на софтуера - минимум 5 (пет) години.	Новите версии на софтуера ще се получават 5 (пет) години.
REQ.224.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.	Обновяването на дефиниции и сигнатури е 5 (пет) години.

1.4.5. Подсистема за централизирано разтоварване на процесите по извършване на динамичен анализ на зловреден код и на кибератаки от другите подсистеми за киберсигурност

Изискано от Възложителя		Предложено от участника
А.		Б.
Общи изисквания		
REQ.225.	Решението трябва да поддържа наблюдение чрез SNMP v3.	Решението поддържа наблюдение чрез SNMP v3. Източник: VX SERIES ADMINISTRATION GUIDE RELEASE 8.3 Страници: 257
REQ.226.	Решението трябва да може да инициализира и използва до 192 виртуални машини едновременно за sandbox анализ, за да може да обработи голям обем от трафик.	Решението може да инициализира и използва до 192 виртуални машини едновременно за sandbox анализ, за да може да обработи голям обем от трафик. Източник: VX SERIES ADMINISTRATION GUIDE RELEASE 8.3
REQ.227.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението трябва да използва собствен, специално изграден хипервайзор.	Решението не използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението използва собствен, специално изграден хипервайзор. Източник: Thinking outside the box - fireeye-outside-sandbox.pdf
REQ.228.	Решението трябва да може да получава автоматично данни за заплахи от засечени такива при други клиенти на вендора от цял свят.	Решението може да получава автоматично данни за заплахи от засечени такива при други клиенти на вендора от цял свят. Източник: VX SERIES ADMINISTRATION GUIDE RELEASE 8.3
REQ.229.	Решението трябва да може да прави анализ на големи файлове до 1024 MB.	Решението може да прави анализ на големи файлове до 1024 MB. Източник: VX SERIES ADMINISTRATION GUIDE RELEASE 8.3

		Страници: 147
REQ.230.	Решението трябва да може да създава локални дефиниции (signatures) на засечените зловредни файлове. Администраторите трябва да могат да конфигурират времето на изтичане на валидността на локалните дефиниции.	Решението може да създава локални дефиниции (signatures) на засечените зловредни файлове. Администраторите могат да конфигурират времето на изтичане на валидността на локалните дефиниции. Източник: VX SERIES ADMINISTRATION GUIDE RELEASE 8.3
REQ.231.	Решението трябва да позволява модифициране на параметрите на Outlook акаунта, използван в sandbox средата.	Решението позволява модифициране на параметрите на Outlook акаунта, използван в sandbox средата. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0107 Страници: 10
REQ.232.	Решението трябва да може да засича webshell скриптове.	Решението може да засича webshell скриптове. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0110 Страници: 9
REQ.233.	Решението трябва да може да изпълнява файлове създадени от MS Office документи в startup директорията на операционната система по време на sandbox анализа.	Решението може да изпълнява файлове създадени от MS Office документи в startup директорията на операционната система по време на sandbox анализа. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0111 Страници: 8
REQ.234.	Решението трябва да може да изпълнява планираните (scheduled) задачи от зловредния код в sandbox средата.	Решението може да изпълнява планираните (scheduled) задачи от зловредния код в sandbox средата.

		Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0110 Страници: 9
REQ.235.	Решението трябва да позволява на администраторите да конфигурират датата и часа (времевата зона) и използвания език в sandbox средата.	Решението позволява на администраторите да конфигурират датата и часа (времевата зона) и използвания език в sandbox средата. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0110 Страници: 9
REQ.236.	Решението трябва да може да извлича URL адреси от паметта по време на sandbox анализа.	Решението може да извлича URL адреси от паметта по време на sandbox анализа. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0109 Страници: 9
REQ.237.	Решението трябва да може да извлича URL адреси от Microsoft Office файлове и от XPS файлове.	Решението може да извлича URL адреси от Microsoft Office файлове и от XPS файлове. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0109 Страници: 9
REQ.238.	Решението трябва да може да извлича и анализира свързани Relationship URL адреси.	Решението може да извлича и анализира свързани Relationship URL адреси. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0103 Страници: 9
REQ.239.	Решението трябва да може да засича зловредни Microsoft Office файлове с вградено видео в тях.	Решението може да засича зловредни Microsoft Office файлове с вградено видео в тях. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0109

		Страници: 9
REQ.240.	Решението трябва да може да извършва анализ на следните специални файлови типове: REG, Microsoft Access, One Note, HTA и Scriptlet.	Решението може да извършва анализ на следните специални файлови типове: REG, Microsoft Access, One Note, HTA и Scriptlet. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0109 Страници: 9 Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0105 Страници: 8 Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0104 Страници: 9 Източник: GUEST IMAGES RELEASE NOTES RELEASE 16.1115 Страници: 9
REQ.241.	Решението трябва да може да анализира Microsoft Office файлове, които са защитени с парола.	Решението може да анализира Microsoft Office файлове, които са защитени с парола. Източник: GUEST IMAGES RELEASE NOTES RELEASE 16.1115 Страници: 9
REQ.242.	Решението трябва да може да засича инжектиране на код.	Решението може да засича инжектиране на код. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0104 Страници: 9

REQ.243.	Решението трябва да може да извършва анализ на файлове използвайки различни версии на Microsoft Office на виртуалните машини за sandbox анализ.	Решението може да извършва анализ на файлове използвайки различни версии на Microsoft Office на виртуалните машини за sandbox анализ. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0107 Страници: 9
REQ.244.	Решението трябва да може да извлича и анализира вградени файлове в Microsoft Office файлове.	Решението може да извлича и анализира вградени файлове в Microsoft Office файлове. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0107 Страници: 9
REQ.245.	Решението трябва да може да наблюдава PowerShell дейностите в sandbox средата и да може да докладва за тях.	Решението може да наблюдава PowerShell дейностите в sandbox средата и може да докладва за тях. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0107 Страници: 9
REQ.246.	Решението трябва да може да извлича файлове, създадени от PowerShell процеси.	Решението може да извлича файлове, създадени от PowerShell процеси. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0107 Страници: 9
REQ.247.	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques) от зловредните процеси, като например PING проверки, проверки за време и техники с диалогови прозорци.	Решението може да се справя с техники за избягване от засичане (evasion techniques) от зловредните процеси, като PING проверки, проверки за време и техники с диалогови прозорци.

		Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0109 Страници: 8 Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0101 Страници: 9
REQ.248.	Решението трябва да може да засича нови криптовируси (ransomware) в sandbox средата – без да има дефиниции (signatures) за тях.	Решението може да засича нови криптовируси (ransomware) в sandbox средата – без да има дефиниции (signatures) за тях. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0102 Страници: 9 Източник: GUEST IMAGES RELEASE NOTES RELEASE 16.0901 Страници: 9
REQ.249.	Решението трябва да поддържа Microsoft Windows 10 за засичане на drive-by атаки.	Решението поддържа Microsoft Windows 10 за засичане на drive-by атаки. Източник: GUEST IMAGES RELEASE NOTES RELEASE 16.0901 Страници: 9
REQ.250.	Решението трябва да може да засича Point of Sale зловредни процеси.	Решението може да засича Point of Sale зловредни процеси. Източник: GUEST IMAGES RELEASE NOTES RELEASE 16.0901 Страници: 9
REQ.251.	Решението трябва да може да засича зловредни процеси, използващи kernel уязвимости.	Решението може да засича зловредни процеси, използващи kernel уязвимости.

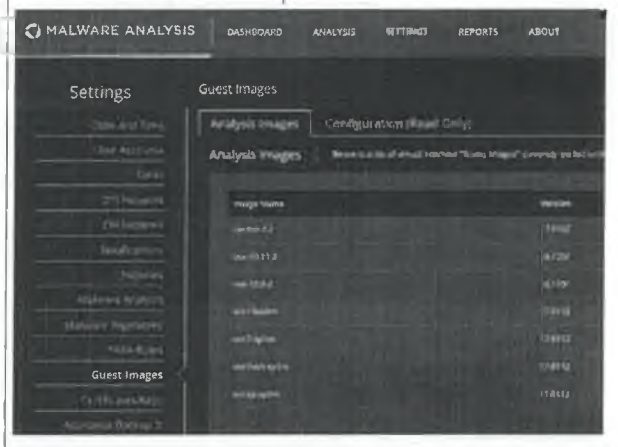
		Източник: GUEST IMAGES RELEASE NOTES RELEASE 16.0901 Страници: 9
REQ.252.	Решението трябва да може да засича DDE атаки.	Решението може да засича DDE атаки. Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0103 Страници: 9
Хардуерни изисквания – 2 броя		**Предложение: 2 броя хардуерни устройства с вграден софтуер FireEye HW-MVX Compute 12550 с включена 5-годишна поддръжка**
REQ.253.	Необходими са 2 броя устройства, които да могат да поемат процесите по анализиране на зловреден код, като по тази начин да може да се увеличи производителността и капацитета на работа на подсистемата за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво, както и да могат да поемат процесите по анализиране при необходимост от подсистемата за динамичен анализ на зловреден код и защита от кибератаки за мрежови файлови дялове, както и от подсистемата за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения, да може да увеличава тяхната производителност и капацитет на работа.	**Предлаганата подсистема за централизирано разтоварване на процесите по извършване на динамичен анализ на зловреден код и на кибератаки от другите подсистеми за киберсигурност включва: 2 броя хардуерни устройства с вграден софтуер FireEye HW-MVX Compute 12550 с включена 5-годишна поддръжка; 2 бр. 5-годишен абонамент FireEye DTI 12550 MVX Compute Off-5Y за прилежащи услуги към хардуерните устройства** https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.254.	Устройството да е с максимална големина 2RU	Устройството е с големина 2RU https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.255.	Устройството да разполага с поне 4TB за съхранение на данни	Устройството разполага с 2 x 4TB за съхранение на данни

		https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.256.	Устройството да разполага минимално със следните портове за свързване с мрежата: 1x 10/100/1000 Mbps BASE-T, 2x 10 Gbps BASE-T, 4x 10GigE SFP+	Устройството разполага със следните портове за свързване с мрежата: 1x 10/100/1000 Mbps BASE-T, 2x 10 Gbps BASE-T, 4x 10GigE SFP https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.257.	Допълнителни портове: 1x 10/100/1000 Mbps BASE-T порт за управление, сериен порт, 2x Type A USB, IPMI, VGA	Устройството разполага със следните допълнителни портове: 1x 10/100/1000 Mbps BASE-T порт за управление, сериен порт, 2x Type A USB, IPMI, VGA https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.258.	Резервирано захранване – 1+1	Устройството разполага с резервирано захранване – 1+1 https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/fireeye-network-threat-prevention-platform.pdf
REQ.259.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.	Устройството работи в изолиран режим, без Интернет свързаност. Устройството не изпраща данни към производителя за засечените заплахи в организацията. Източник: DTI UPDATE PORTAL USER GUIDE RELEASE 1.4.1 Източник: OLP_UG_1.4.1_en.pdf

		Страници: 22
Гаранция и поддръжка:		**Предлагана гаранция и поддръжка от производителя:**
REQ.260.	Срок на хардуерната гаранция - минимум 5 (пет) години.	Срокът на хардуерната гаранция е 5 (пет) години.
REQ.261.	Срок на техническа поддържка – минимум 5 (пет) години.	Срокът на техническа поддръжка е 5 (пет) години.
REQ.262.	Получаване на нови версии на софтуера - минимум 5 (пет) години.	Новите версии на софтуера ще се получават 5 (пет) години.
REQ.263.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.	Обновяването на дефиниции и сигнатури е 5 (пет) години.

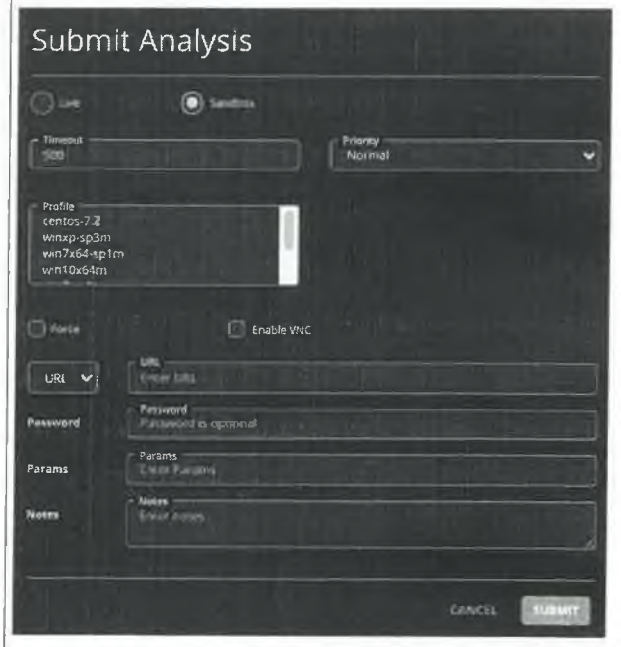
1.4.6. Подсистема (лаборатория) за динамичен анализ на зловреден код

Изискано от Възложителя		**Предложено от участника**
А.		**Б.**
Общи изисквания		
REQ.264.	Тип решение: 1 брой хардуер с вграден софтуер и 5-годишна поддръжка, 5-годишен абонамент за прилежащи услуги	Предлаганата подсистема (лаборатория) за динамичен анализ на зловреден код включва: **1 брой хардуерно устройство с вграден софтуер FireEye 5550AX-HW MAS с включена 5-годишна поддръжка; 1 бр. 5-годишен абонамент FireEye DTI AX 5550 Off sub-5Y за прилежащи услуги към хардуерното устройство**
REQ.265.	Решението трябва да предоставя на анализаторите на сигурността защитена среда, в която те да могат да тестват, стартират и документират процесите на сложни зловредни кодове (malware), като да се предоставят голям набор от виртуални машини, с предварително инсталирани операционни системи и софтуер, бивайки Windows OS (включително XP, 7, 10),	Решението предоставя на анализаторите на сигурността защитена среда, в която те могат да тестват, стартират и документират процесите на сложни зловредни кодове (malware), като се предоставят голям набор от виртуални машини, с предварително инсталирани операционни системи и софтуер, бивайки Windows OS (включително XP, 7, 10), Mac OSX и Linux Cent OS, като могат да се

	Mac OSX и Linux Cent OS, като да могат да се стартират и използват поне 30 виртуални машини едновременно.	стартират и използват поне 30 виртуални машини едновременно. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/forensics/ds-malware-analysis.pdf 
REQ.266.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението трябва да използва собствен, специално изграден хипервайзор.	Решението не използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението използва собствен, специално изграден хипервайзор. Източник: Thinking outside the box - fireeye-outside-sandbox.pdf
REQ.267.	Виртуалните машини, които ще се използват за анализа, трябва да имат инсталирани най-базовите браузъри (минимално Internet Explorer, Microsoft Edge, Mozilla Firefox, Google	Виртуалните машини, които ще се използват за анализа, имат инсталирани най-базовите браузъри (Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome, Safari), плъгини (Adobe Flash) и

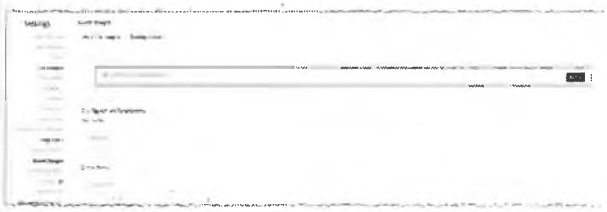
	Chrome, Safari), плъгини (минимално Adobe Flash) и други необходими приложения от трети разработчици (минимално Adobe Reader , VLC, QuickTime, Real Player, Microsoft Office Word, Excel, Powerpoint, Preview).	други необходими приложения от трети разработчици (Adobe Reader , VLC, QuickTime, Real Player, Microsoft Office Word, Excel, Powerpoint, Preview). Източник: AX platform.docx
REQ.268.	Лицензите за операционните системи и за комерсиалните приложения на предварително създадените и конфигурирани виртуални машини трябва да бъдат предоставени от вендора на решението за динамичен анализ.	Лицензите за операционните системи и за комерсиалните приложения на предварително създадените и конфигурирани виртуални машини са предоставени от вендора на решението за динамичен анализ. Източник: AX_UG_8.4.0_en.pdf Страници: 23
REQ.269.	Решението трябва да позволява автоматичното възстановяване на виртуалните машини за анализ към предварително конфигурираното им базово състояние, веднага щом приключи анализа на подадена проба от зловреден код.	Решението позволява автоматичното възстановяване на виртуалните машини за анализ към предварително конфигурираното им базово състояние, веднага щом приключи анализа на подадена проба от зловреден код. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/forensics/ds-malware-analysis.pdf
REQ.270.	Решението трябва да позволява взаимодействие от анализаторите с виртуалните машини по време на динамичния анализ.	Решението позволява взаимодействие от анализаторите с виртуалните машини по време на динамичния анализ. Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4 **Страници: 128**

REQ.271.	Решението трябва да може да извъшрва анализ на поне следните файлови типове: 7zip, zip, rar, gz, 3gp, accdb, app, apk, applet, asf, asp, aspx, avi, bat, cdf, chm, cmd, com, csv , dll, dmg, doc, docx, eeml, elf, eml, exe, flv, gen, gif, hlp, hta, htm, ico, inf, inf64, jar, jpeg, jpg, js, jsp, lnk, mach-o , midi, mov, mp3, mp4, mpg, mpkg, msg, msi, one, onepkg, pdf, php, pkg, pl, png, ppsx, ppt, pptx, ps1, pub, py, pyc, qt, raw32, raw64 , rb, reg, rm, rmi, rtf, sct, sh, swf, swf built-in swf, tiff, url, url-applet, vbs, vcf, vcs, war, wav, wma, wsf, xdp, xls, xlsx, xml, xsl, shell скриптове ако са уеб-базирани (Python, Perl, Ruby), txt.	Решението може да извършва анализ на следните файлови типове: 7zip, zip, rar, gz, 3gp, accdb, app, apk, applet, asf, asp, aspx, avi, bat, cdf, chm, cmd, com, csv , dll, dmg, doc, docx, eeml, elf, eml, exe, flv, gen, gif, hlp, hta, htm, ico, inf, inf64, jar, jpeg, jpg, js, jsp, lnk, mach-o , midi, mov, mp3, mp4, mpg, mpkg, msg, msi, one, onepkg, pdf, php, pkg, pl, png, ppsx, ppt, pptx, ps1, pub, py, pyc, qt, raw32, raw64 , rb, reg, rm, rmi, rtf, sct, sh, swf, swf built-in swf, tiff, url, url-applet, vbs, vcf, vcs, war, wav, wma, wsf, xdp, xls, xlsx, xml, xsl, уеб-базирани shell скриптове (Python, Perl, Ruby), txt. Източник: AX platform.docx
REQ.272.	Решението трябва да може да прави анализ на големи файлове до 1024 MB.	Решението може да прави анализ на големи файлове до 1024 MB. Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4 Страници: 78
REQ.273.	Решението трябва да може да извършва статичен и динамичен анализ по поне следните методи: YARA, сканиране с антивирусни дефиниции, Python-базиран статичен анализ, засичане на dropper процеси, анализ на URL адреси, които са вградени във файлове и електронни съобщения, анализ на riskware, анализ на динамичните процеси във виртуалните машини.	Решението може да извършва статичен и динамичен анализ по следните методи: YARA, сканиране с антивирусни дефиниции, Python-базиран статичен анализ, засичане на dropper процеси, анализ на URL адреси, които са вградени във файлове и електронни съобщения, анализ на riskware, анализ на динамичните процеси във виртуалните машини. Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4

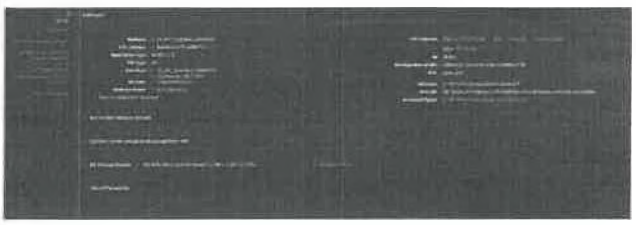
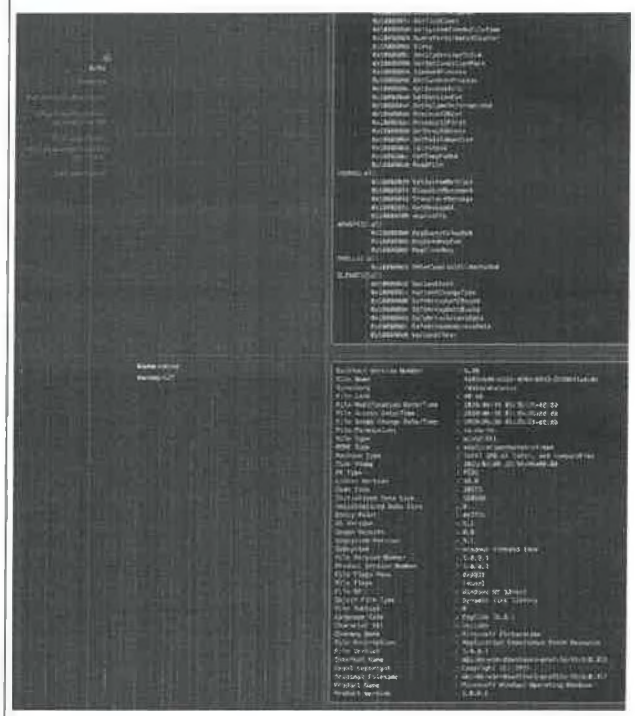
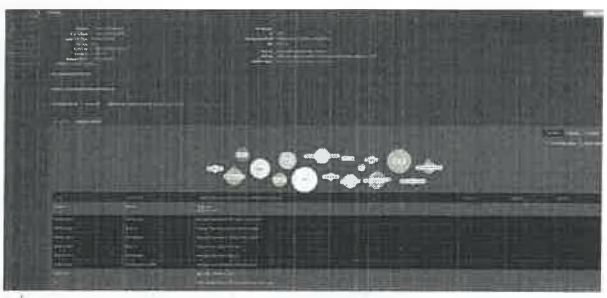
		Страници: 33, 51-59
REQ.274.	Решението трябва да може да анализира целия жизнен цикъл на дадена кибератака, започвайки от първоначалното проникване в системата (exploit), свързвания с хакерски команден център и сваляне на вторични зловредни модули.	Решението може да анализира целия жизнен цикъл на дадена кибератака, започвайки от първоначалното проникване в системата (exploit), свързвания с хакерски команден център и сваляне на вторични зловредни модули. Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4 Страници: 131
REQ.275.	Решението трябва да позволява сравнението на поведението на анализирания зловреден код под различните конфигурации на средата за анализ (при различни версии на Microsoft Windows и Mac OSX операционни системи, различни версии на инсталираните приложения, различни настройки на операционните системи, при различни приложени обновления на операционните системи, при приложени различни кръпки и Service Pack версии).	Решението позволява сравнението на поведението на анализирания зловреден код под различните конфигурации на средата за анализ (при различни версии на Microsoft Windows и Mac OSX операционни системи, различни версии на инсталираните приложения, различни настройки на операционните системи, при различни приложени обновления на операционните системи, при приложени различни кръпки и Service Pack версии). Източник: AX platform.docx 

REQ.276.	Предложеното решение трябва да дава възможно най-малко грешни показания и да вдига възможно най-малко грешни аларми при засичането на файлове, които наподобяват зловреден код: да алармира за поведение, което опитва да избегне засичане от системите за сигурност, инсталиране на нежелани програми, промяна на системните настройки, което влошава производителността на системите, наличие на потенциално нежелани програми (PUP) и на потенциално нежелани приложения (PUA), adware процеси и използване на инструменти, които често се използват от атакуващи хакери.	Предложеното решение дава възможно най-малко грешни показания и вдига възможно най-малко грешни аларми при засичането на файлове, които наподобяват зловреден код: алармира за поведение, което опитва да избегне засичане от системите за сигурност, инсталиране на нежелани програми, промяна на системните настройки, което влошава производителността на системите, наличие на потенциално нежелани програми (PUP) и на потенциално нежелани приложения (PUA), adware процеси и използване на инструменти, които често се използват от атакуващи хакери. Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4 Страници: 70
REQ.277.	Решението трябва да позволява едновременното използване на няколко виртуални машини за анализ, където различни зловредни приложения да могат да бъдат анализирани по едно и също време, без да взаимодействат помежду си.	Решението позволява едновременното използване на няколко виртуални машини за анализ, където различни зловредни приложения могат да бъдат анализирани по едно и също време, без да взаимодействат помежду си. Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4 **Страници: 121**
REQ.278.	Решението трябва да може да симулира човешки действия по виртуалните машини за анализ, така че дори зловредните приложения,	Решението може да симулира човешки действия по виртуалните машини за анализ, така че дори зловредните приложения, които имат проверки в

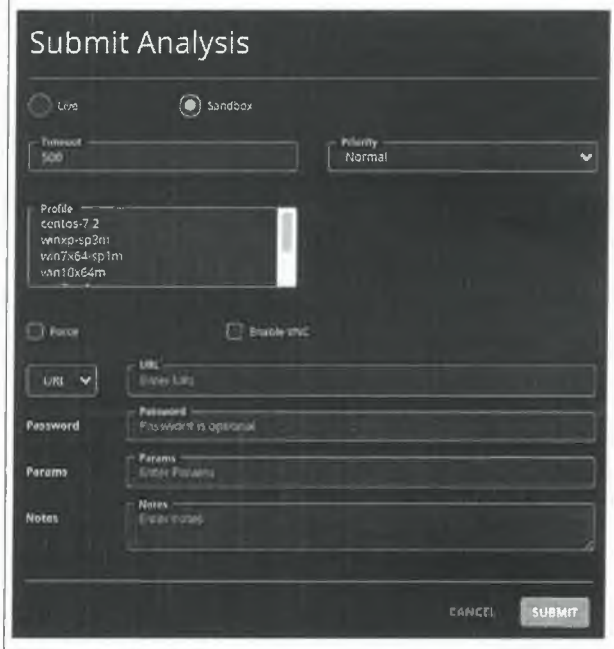
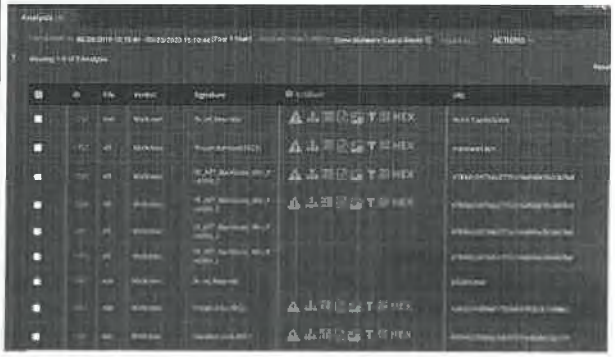
	които имат проверки в себе си дали в момента взаимодействат с реален потребител (извиквайки някои вградени функции на Windows или от Windows API интерфейса), да се изпълнят напълно и да могат да бъдат анализирани.	себе си дали в момента взаимодействат с реален потребител (извиквайки някои вградени функции на Windows или от Windows API интерфейса), се изпълнят напълно и да могат да бъдат анализирани. Източник: fireeye-hot-knives-through-butter.pdf
REQ.279.	По време на извършване на анализа във виртуалните машини, решението трябва да може да се справя с опити от зловредния код за избягване на засичане, като например използване на ping командите, проверка на домейна, проверка на отметките в браузърите, проверка на Outlook акаунтите, проверка на активните процеси, верифициране DNS.	По време на извършване на анализа във виртуалните машини, решението може да се справя с опити от зловредния код за избягване на засичане, като използване на ping командите, проверка на домейна, проверка на отметките в браузърите, проверка на Outlook акаунтите, проверка на активните процеси, верифициране DNS. Източник: fireeye-hot-knives-through-butter.pdf Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0109 Страници: 8 Източник: GUEST IMAGES RELEASE NOTES RELEASE 17.0101 Страници: 9
REQ.280.	Решението трябва да може автоматично да взаимодейства със зловредни приложения, които използват графичен интерфейс и които изискват взаимодействие с извикани диалогови прозорци или с извършване на стъпки по инсталирането на приложения.	Решението може автоматично да взаимодейства със зловредни приложения, които използват графичен интерфейс и които изискват взаимодействие с извикани диалогови прозорци или с извършване на стъпки по инсталирането на приложения. Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4

		Страници: 128
REQ.281.	Решението трябва да позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите трябва да могат да променят поне следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, наскоро достъпени файлове, DNS записи.	Решението позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите могат да променят следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, наскоро достъпени файлове, DNS записи. Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4 Страници: 128 
REQ.282.	Решението трябва да позволява създаването на подробни технически отчети, които да съдържат информация за анализираните файлове, като например; • Типа на анализирания файл; • Контролните суми (MD5, SHA) на анализираните файлове / създадените файлове на виртуалните машини за анализ; • Проверка с YARA правила; • Инстинкия тип на анализирания файл; • MD5 и SHA1 стойности на първоначалния обект, но също и на всеки друг обект създаден от него; • Използваните DLL библиотеки, респективно функциите използвани от	Решението позволява създаването на подробни технически отчети, които съдържат информация за анализираните файлове, като: • Типа на анализирания файл; • Контролните суми (MD5, SHA) на анализираните файлове / създадените файлове на виртуалните машини за анализ; • Проверка с YARA правила; • Инстинкия тип на анализирания файл; • MD5 и SHA1 стойности на първоначалния обект, но също и на всеки друг обект създаден от него; • Използваните DLL библиотеки, респективно функциите използвани от зловредния код, излвечени от IAT таблицата;

	зловредния код, излвечени от IAT таблицата; • Датата на компилиране на файла; • Направените промени на ниво инсталираните приложения на системите за анализ; • Промени по файловата система; • Направените промени по Windows Registry базата от данни; • Извиканите Windows API функции, в хронологичен ред; • Информация за създадените / модифицираните / спрените процеси; • Информация за създадените / модифицираните / спрените Windows услуги (services); • Създадените Mutex обекти; • За всички създадени SSDT, IDT, IRP Hooks; • Направени мрежови свързвания и използвани транспортни мрежови протоколи; • Уловен мрежови трафик (под формата на PCAP файл), произтичащ от системата за анализ; • DNS заявки; • Достъпени IP адреси и използвани логически портове; • Уловени съмнителни процеси на виртуалната машина при анализа; • Записани screenshots / видео, направени по време на анализа на зловредните приложения;	• Датата на компилиране на файла; • Направените промени на ниво инсталираните приложения на системите за анализ; • Промени по файловата система; • Направените промени по Windows Registry базата от данни; • Извиканите Windows API функции, в хронологичен ред; • Информация за създадените / модифицираните / спрените процеси; • Информация за създадените / модифицираните / спрените Windows услуги (services); • Създадените Mutex обекти; • За всички създадени SSDT, IDT, IRP Hooks; • Направени мрежови свързвания и използвани транспортни мрежови протоколи; • Уловен мрежови трафик (под формата на PCAP файл), произтичащ от системата за анализ; • DNS заявки; • Достъпени IP адреси и използвани логически портове; • Уловени съмнителни процеси на виртуалната машина при анализа; • Записани screenshots / видео, направени по време на анализа на зловредните приложения; • Типа на използваните уязвимости (exploits) от зловредния код.

	• Типа на използваните уязвимости (exploits) от зловредния код.	Източник: AX platform.docx Източник: submission_by_id_ax02_20200620_ 1441457606505010 00.pdf   
REQ.283.	Решението трябва да може да издава отчети в следните формати: PDF, CSV, Text, JSON, XML.	Решението може да издава отчети в следните формати: PDF, CSV, Text, JSON, XML.

		Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4 **Страници: 156**
REQ.284.	Решението трябва да използва специално заделен мрежови интерфейс когато е пуснато в „жив" режим, за да се избегне допускането на зловреден мрежови трафик към реалната вътрешна мрежа на организацията; Мрежовият интерфейс трябва да позволява на зловредния код да достъпва външни хакерски командни сървъри и да сваля всички допълнителни модули и артефакти, които са му необходими, за да се изпълни изцяло за анализ, включително когато мрежата е конфигурирана да използва уеб прокси.	Решението използва специално заделен мрежови интерфейс когато е пуснато в „жив" режим, за да се избегне допускането на зловреден мрежови трафик към реалната вътрешна мрежа на организацията; Мрежовият интерфейс позволява на зловредния код да достъпва външни хакерски командни сървъри и да сваля всички допълнителни модули и артефакти, които са му необходими, за да се изпълни изцяло за анализ, включително когато мрежата е конфигурирана да използва уеб прокси. **Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4** **Страници: 123**
REQ.285.	Решението не трябва да позволява мрежови комуникации от виртуалните системи/sandbox за анализ към Интернет, когато решението е пуснато в Sandbox режим: зловредния код във виртуалните машини не трябва да може да комуникира с хакерски командни центрове или URL адреси в Интернет в този режим.	Решението не позволява мрежови комуникации от виртуалните системи/sandbox за анализ към Интернет, когато решението е пуснато в Sandbox режим: зловредния код във виртуалните машини не може да комуникира с хакерски командни центрове или URL адреси в Интернет в този режим. Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4 Страници: 20
REQ.286.	Решението трябва да може да засича когато зловредния код извиква sleep функции и да поставя времева точка в бъдещето, която да отговори на условието за изпълнение. Да може да симулира човешки действия като например кликване с мишката, за да може да стартира	Решението може да засича когато зловредния код извиква sleep функции и да поставя времева точка в бъдещето, която да отговори на условието за изпълнение. Решението може да симулира човешки действия като например кликване с мишката, за да може да стартира такъв тип зловреден код, използващ такива критерии.

	такъв тип зловреден код, използващ такива критерии.	Източник: fireeye-hot-knives-through-butter.pdf
REQ.287.	Решението да позволява на администраторите да могат да избират с кои приложения да се стартира анализа в дадена виртуалната машина.	Решението позволява на администраторите да избират с кои приложения да се стартира анализа в дадена виртуалната машина. Източник: AX platform.docx 
REQ.288.	Решението трябва да може да разпознава зловредно поведение от общ характер, както и да класифицира зловредните приложения от дадено семейство вируси (троянски кон, keylogger, rootkit, RAT и т.н.) по наблюдавания модел на поведение.	Решението може да разпознава зловредно поведение от общ характер, както и да класифицира зловредните приложения от дадено семейство вируси (троянски кон, keylogger, rootkit, RAT и т.н.) по наблюдавания модел на поведение. 

REQ.289.	Решението трябва да може да използва YARA правила за разпознаване на зловреден код.	Решението може да използва YARA правила за разпознаване на зловреден код. Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4 Страници: 33
REQ.290.	Решението трябва да може да се свързва с файлови сървъри, използвайки протоколите Server Message Block или Internet File System, за анализ на съхранени файлове.	Решението може да се свързва с файлови сървъри, използвайки протоколите Server Message Block или Internet File System, за анализ на съхранени файлове. Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4 Страници: 149
REQ.291.	Решението трябва да позволява конфигурирането на различни споделени файлови директории, в зависимост от операционната система, която ще се използва за извършването на анализ на зловреден код.	Решението позволява конфигурирането на различни споделени файлови директории, в зависимост от операционната система, която ще се използва за извършването на анализ на зловреден код. Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4 Страници: 147, 151
REQ.292.	Решението трябва да може автоматично да разпределя анализираните файлове към различни локации, използвайки споделени мрежови дялове, според това дали имат зловредно поведение или нямат зловредно поведение.	Решението може автоматично да разпределя анализираните файлове към различни локации, използвайки споделени мрежови дялове, според това дали имат зловредно поведение или нямат зловредно поведение. Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4 Страници: 147, 151
REQ.293.	Решението трябва да може да изпраща автоматични известия чрез Syslog, HTTP, SNMP и SMTP протоколи.	Решението може да изпраща автоматични известия чрез Syslog, HTTP, SNMP и SMTP протоколи.

		Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4 Страници: 83
REQ.294.	Решението трябва да позволява избирането на времевия интервал, през който да бъдат проверявани споделените дялове за нови файлове.	Решението позволява избирането на времевия интервал, през който да бъдат проверявани споделените дялове за нови файлове. Източник: MALWARE ANALYSIS USER GUIDE RELEASE 8.4 Страници: 147
REQ.295.	Решението трябва да може да използва прокси с автентикация за достъпване на сървъра му за обновления.	Решението може да използва прокси с автентикация за достъпване на сървъра му за обновления. Източник: MALWARE ANALYSIS SYSTEM ADMINISTRATION GUIDE RELEASE 8.4
REQ.296.	Решението трябва да работи с уеб-базирана конзола за управление, която да не изисква инсталирането на допълнителен софтуер за достъпването ѝ.	Решението работи с уеб-базирана конзола за управление, която не изисква инсталирането на допълнителен софтуер за достъпването ѝ. Източник: MALWARE ANALYSIS SYSTEM ADMINISTRATION GUIDE RELEASE 8.4 Страници: 23
REQ.297.	Решението трябва да позволява конфигурирането на ACL списък, за да се ограничат позволените свързвания с интерфейса за управление.	Решението позволява конфигурирането на ACL списък, за да се ограничат позволените свързвания с интерфейса за управление. Източник: MALWARE ANALYSIS SYSTEM ADMINISTRATION GUIDE RELEASE 8.4 Страници: 151
REQ.298.	Решението трябва да използва криптиран канал за комуникация между администраторите и конзолата за управление. Също така, трябва да позволява вмъкването на собствени дигитални	Решението използва криптиран канал за комуникация между администраторите и конзолата за управление. Решението позволява вмъкването на собствени дигитални сертификати на

	сертификати на организацията, използвани за криптиране на връзката.	организацията, използвани за криптиране на връзката. Източник: FireEye AX System Administration Guide 8.4.0 Страници: 111-112
REQ.299.	Решението трябва да позволява локално задаване на дата и час или чрез синхронизация с NTP сървър.	Решението позволява локално задаване на дата и час или чрез синхронизация с NTP сървър. Източник: FireEye AX System Administration Guide 8.4.0 Страници: 129
REQ.300.	Решението трябва да позволява създаването на акаунти с различни роли и права, например администратори и потребители, които само следят за аларми.	Решението позволява създаването на акаунти с различни роли и права, като администратори и потребители, които само следят за аларми. Източник: FireEye AX System Administration Guide 8.4.0 Страници: 111 Източник: SYSTEM SECURITY SYSTEM SECURITY GUIDE RELEASE 2019.4 Страници: 421
REQ.301.	Решението трябва да позволява автентикиране към конзолата за управление чрез RADIUS, TACACS + и LDAP.	Решението позволява автентикиране към конзолата за управление чрез RADIUS, TACACS + и LDAP. Източник: SYSTEM SECURITY SYSTEM SECURITY GUIDE RELEASE 2019.4 Страници: 57
REQ.302.	Решението трябва да може автоматично да изпраща известия и периодично създадени отчети за „здравето“ си, използвайки SMTP.	Решението може автоматично да изпраща известия и периодично създадени отчети за „здравето“ си, използвайки SMTP. Източник: FireEye AX System Administration Guide 8.4.0 Страници: 113-114

REQ.303.	Решението трябва да позволява извличането на аларми и отчети за активността на зловреден код под формата на PDF.	Решението позволява извличането на аларми и отчети за активността на зловреден код под формата на PDF.
REQ.304.	Решението трябва да позволява конфигурирането на съобщение, което да се показва при вписване в конзолата за управление.	Решението позволява конфигурирането на съобщение, което да се показва при вписване в конзолата за управление. Източник: FireEye AX System Administration Guide 8.4.0 Страници: 232
REQ.305.	Решението трябва да може да се интегрира със специализирано оборудване за централизирано управление, което да може да корелира резултатите от анализите и да разпространява индикаторите за компроментиране до другите подсистеми за анализ на зловреден код.	Решението може да се интегрира със специализирано оборудване за централизирано управление, което може да корелира резултатите от анализите и да разпространява индикаторите за компроментиране до другите подсистеми за анализ на зловреден код. Източник: CENTRAL MANAGEMENT ADMINISTRATION GUIDE RELEASE 8.7 Страници: 507
REQ.306.	Решението трябва да може да се интегрира с Endpoint Detection and Response системи, като да може да получава артефакти от зловреден код уловен от софтуерните агенти на такъв тип система, инсталирани на ниво крайна точка или сървър.	Решението може да се интегрира с Endpoint Detection and Response системи, като може да получава артефакти от зловреден код уловен от софтуерните агенти на такъв тип система, инсталирани на ниво крайна точка или сървър. Източник: ENDPOINT SECURITY ENDPOINT ENRICHER MODULE USER GUIDE Страници: 5

[redacted] [redacted]

REQ.307.	Решението трябва да може лесно да се интегрира с други подсистеми за мрежова защита и за email защита, за да се предостави информация в реално време за зловредни мрежови заявки (callbacks) и за споделяне на локално генерираните индикатори за компроментиране от анализите.	Решението може лесно да се интегрира с други подсистеми за мрежова защита и за email защита, за да се предостави информация в реално време за зловредни мрежови заявки (callbacks) и за споделяне на локално генерираните индикатори за компроментиране от анализите. Източник: CENTRAL MANAGEMENT ADMINISTRATION GUIDE RELEASE 8.7 Страници: 507
Хардуерни изисквания – 1 брой		**Предложение: 1 брой хардуерно устройство с вграден софтуер FireEye 5550AX-HW MAS с включена 5-годишна поддръжка**
REQ.308.	Устройството да е с максимална големина 1RU	Устройството е с големина 1RU https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/forensics/ds-malware-analysis.pdf
REQ.309.	Устройството да разполага с поне 4TB за съхранение на данни	Устройството разполага с 2 x 4TB за съхранение на данни https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/forensics/ds-malware-analysis.pdf

REQ.310.	Устройството да разполага минимално със следните портове за свързване с мрежата: 2x 10/100/1000BASE-T Ports	Устройството разполага със следните портове за свързване с мрежата: 2x 10/100/1000BASE-T Ports https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/forensics/ds-malware-analysis.pdf
REQ.311.	Допълнителни портове: сериен порт, 4x Type A USB, IPMI, VGA	Устройството разполага със следните допълнителни портове: сериен порт, 4x Type A USB, IPMI, VGA https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/forensics/ds-malware-analysis.pdf
REQ.312.	Резервирано захранване – 1+1	Устройството разполага с резервирано захранване – 1+1 https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/forensics/ds-malware-analysis.pdf
REQ.313.	Устройството да може да извършва минимално 8200 анализа на ден.	Устройството може да извършва 8200 анализа на ден. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/forensics/ds-malware-analysis.pdf
REQ.314.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.	Устройството работи в изолиран режим, без Интернет свързаност. Устройството не изпраща данни към производителя за засечените заплахи в организацията. Източник: DTI UPDATE PORTAL USER GUIDE RELEASE 1.4.1

		Източник: OLP_UG_1.4.1_en.pdf Страници: 22
Гаранция и поддръжка:		**Предлагана гаранция и поддръжка от производителя:**
REQ.315.	Срок на хардуерната гаранция - минимум 5 (пет) години.	Срокът на хардуерната гаранция е 5 (пет) години.
REQ.316.	Срок на техническа поддържка – минимум 5 (пет) години.	Срокът на техническа поддръжка е 5 (пет) години.
REQ.317.	Получаване на нови версии на софтуера - минимум 5 (пет) години.	Новите версии на софтуера ще се получават 5 (пет) години.
REQ.318.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.	Обновяването на дефиниции и сигнатури е 5 (пет) години.

1.4.7. Подсистема за динамичен анализ на зловреден код и защита от кибератаки за мрежови файлови дялове (лаборатория) за динамичен анализ на зловреден код

Изискано от Възложителя		**Предложено от участника**
А.		**Б.**
Общи изисквания		
REQ.319.	Тип решение: 1 брой хардуер с вграден софтуер и 5-годишна поддръжка, 5-годишен абонамент за прилежащи услуги	Предлаганата подсистема за динамичен анализ на зловреден код и защита от кибератаки за мрежови файлови дялове (лаборатория) за динамичен анализ на зловреден код включва: **1 брой хардуерно устройство с вграден софтуер FireEye HW-6500 FX с включена 5-годишна поддръжка; 1 бр. 5-годишен абонамент FireEye DTI 6500 FX Off-5Y за прилежащи услуги към хардуерното устройство**
REQ.320.	Решението трябва да може да анализира файлове, използвайки sandbox технология,	Решението може да анализира файлове, използвайки sandbox технология, която може да засича непознат „zero-day" зловреден код, вграден във файловете.

[redacted] [redacted]

	която да може да засича непознат „zero-day" зловреден код, вграден във файловете.	Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 17
REQ.321.	Решението трябва да може да получава автоматично данни за заплахи от засечени такива при други клиенти на вендора от цял свят.	Решението може да получава автоматично данни за заплахи от засечени такива при други клиенти на вендора от цял свят. Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 75
REQ.322.	Решението трябва да може да извършва рекурсивни автоматични сканирания, сканирания по времеви график и сканирания по ръчна заявка от администратор, за всички достъпни мрежови файлови дялове, за да да може да идентифицира и сложи под карантина всички засечени вируси по съхранените файлове, без да има значително влияние върху производителността на системите.	Решението може да извършва рекурсивни автоматични сканирания, сканирания по времеви график и сканирания по ръчна заявка от администратор, за всички достъпни мрежови файлови дялове, за да идентифицира и сложи под карантина всички засечени вируси по съхранените файлове, без да има значително влияние върху производителността на системите. Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 17, 131
REQ.323.	Решението да позволява задаването на различни настройки за всяко сканиране, като да могат да се задават различни файлови типове или конкретни файлове да могат да бъдат сложени в „бял списък", за да са изключени от сканирането.	Решението позволява задаването на различни настройки за всяко сканиране, като могат да се задават различни файлови типове или конкретни файлове могат да бъдат сложени в „бял списък", за да са изключени от сканирането. Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 134

REQ.324.	Решението трябва да позволява паузиране и продължаване на сканирания, които се извършват в даден момент (в реално време).	Решението позволява паузиране и продължаване на сканирания, които се извършват в даден момент (в реално време). **Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3** **Страници: 143**
REQ.325.	Решението трябва да може да премества безопасните файлове в определени локации, а заразените файлове да може да премества в отделена карантина.	Решението може да премества безопасните файлове в определени локации, а заразените файлове може да премества в отделена карантина. Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 122
REQ.326.	Решението трябва да може да връща файлове в първоначалните им локации, след като са освободени от карантината.	Решението може да връща файлове в първоначалните им локации, след като са освободени от карантината. Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 **Страници: 164**
REQ.327.	Решението трябва да може да издава пълни отчети за поведението на файловете – прилежащи процеси, достъп до файловете/записани файлове на дисковото пространство, промени в регистрите на операционната система.	Решението може да издава пълни отчети за поведението на файловете – прилежащи процеси, достъп до файловете/записани файлове на дисковото пространство, промени в регистрите на операционната система. **Източник: FILE PROTECT USER GUIDE RELEASE 8.3** Страници: 20
REQ.328.	Решението трябва да може да споделя откритите от него индикатори за компроментиране с останалите подсистеми, за	Решението може да споделя откритите от него индикатори за компроментиране с останалите подсистеми, за динамичен анализ на зловреден

	динамичен анализ на зловреден код и за разследвания за кибератаки, също така да може и да получава индикатори за компроментиране от тях.	код и за разследвания за кибератаки, също така може и да получава индикатори за компроментиране от тях. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 20-22
REQ.329.	Решението трябва да предоставя настройки на филтри при сканирането на файлове, според типа на файловете, локацията им, последната дата на модифициране.	Решението предоставя настройки на филтри при сканирането на файлове, според типа на файловете, локацията им, последната дата на модифициране. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 136
REQ.330.	Решението трябва да позволява използването на YARA правила, версия 3.4.	Решението позволява използването на YARA правила, версия 3.4. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 28
REQ.331.	Решението трябва да може да извършва освен динамичен анализ, така и статичен анализ. Администраторите трябва да могат да избират дали да се извършва статичния анализ.	Решението може да извършва освен динамичен анализ, така и статичен анализ. Администраторите могат да избират дали да се извършва статичния анализ.

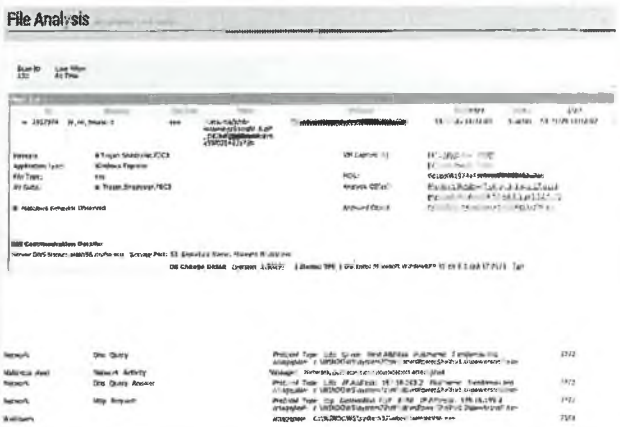
		Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 37
REQ.332.	Решението трябва да може да анализира файлове с големина до поне 1024 MB. Максималният размер на файловете, които ще се анализират, да може да бъде променян.	Решението може да анализира файлове с големина до поне 1024 MB. Максималният размер на файловете, които ще се анализират, може да бъде променян. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 53
REQ.333.	Решението трябва да може да прави морфологичен разбор на .eml файлове.	Решението може да прави морфологичен разбор на .eml файлове. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 56
REQ.334.	Решението трябва да може да извлича прикачени файлове от .eml файлове. Броя на прикачени файлове, които да се анализират, трябва да може да бъде променян.	Решението може да извлича прикачени файлове от .eml файлове. Броя на прикачени файлове, които да се анализират, може да бъде променян. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 56
REQ.335.	Решението трябва да може да създава локални дефиниции (signatures) на засечените зловредни файлове след динамичен анализ. Администраторите трябва да могат да конфигурират времето на изтичане на валидността на локалните дефиниции.	Решението може да създава локални дефиниции (signatures) на засечените зловредни файлове след динамичен анализ. Администраторите могат да конфигурират времето на изтичане на валидността на локалните дефиниции. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 57
REQ.336.	Решението трябва да може да се интегрира по подразбиране с Microsoft Office 365 за обработка на файлове.	Решението може да се интегрира по подразбиране с Microsoft Office 365 за обработка на файлове. Източник: FILE PROTECT USER GUIDE RELEASE 8.

		Страници: 60
REQ.337.	Решението трябва да може да се интегрира по подразбиране с Microsoft OneDrive за обработка на файлове. Решението трябва да може да извършва динамичен анализ на файловете в облачното пространство на OneDrive.	Решението може да се интегрира по подразбиране с Microsoft OneDrive за обработка на файлове. Решението може да извършва динамичен анализ на файловете в облачното пространство на OneDrive. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 67
REQ.338.	Решението трябва да може да се интегрира по подразбиране с Microsoft SharePoint Online, за защитено споделяне на файлове.	Решението може да се интегрира по подразбиране с Microsoft SharePoint Online, за защитено споделяне на файлове. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 74
REQ.339.	Решението трябва да може да изпраща известия за събития по email, HTTP, Rsyslog, SNMP в XML, JSON или в текстов формат.	Решението може да изпраща известия за събития по email, HTTP, Rsyslog, SNMP в XML, JSON, в текстов формат. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 82
REQ.340.	Решението трябва да поддържа следните протоколи: CIFS, NFS, WebDAV, Secure WebDAV.	Решението поддържа следните протоколи: CIFS, NFS, WebDAV, Secure WebDAV. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 122
REQ.341	Решението трябва да позволява избирането на кои файлови хранилища да се сканират, директно от графичния интерфейс за управление.	Решението позволява избирането на кои файлови хранилища да се сканират, директно от графичния интерфейс за управление. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 124

REQ.342.	Решението трябва да може да извлича първоначална информация за споделените дискови пространства, като например брой и тип на файловете на тях, за да може по-лесно да се определят критериите за сканирането им от решението.	Решението може да извлича първоначална информация за споделените дискови пространства, като брой и тип на файловете на тях, за да може по-лесно да се определят критериите за сканирането им от решението. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 131
REQ.343.	Решението трябва да предоставя информация за резултатите след извършване на сканиране.	Решението предоставя информация за резултатите след извършване на сканиране. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 156
REQ.344.	Решението трябва да може да предоставя детайлни отчети във формати .xml, .json, .csf и текстов формат, както и обобщителни отчети в .pdf формат.	Решението може да предоставя детайлни отчети във формати .xml, .json, .csf и текстов формат, както и обобщителни отчети в .pdf формат. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 176
REQ.345.	Решението трябва да позволява определянето на времеви график за автоматично изготвяне и изпращане на отчети.	Решението позволява определянето на времеви график за автоматично изготвяне и изпращане на отчети. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 181, 190
REQ.346.	Решението трябва да позволява лесно извличане на резултати от анализи в PDF формат.	Решението позволява лесно извличане на резултати от анализи в PDF формат. Източник: FILE PROTECT USER GUIDE RELEASE 8.3 Страници: 30
REQ.347.	Решението трябва да поддържа ролево-базиран достъп до конзолата за управление.	Решението поддържа ролево-базиран достъп до конзолата за управление.

		Източник: SYSTEM SECURITY SYSTEM SECURITY GUIDE RELEASE 2019.4 Страници: 373
REQ.348.	Решението трябва да може да се интегрира с подистемата за централизирано управление и да може да се конфигурира от нея. Трябва да могат да се получават системни обновления през подсистемата за централизирано управление и да се обменят аларми и известия.	Решението може да се интегрира с подистемата за централизирано управление и може да се конфигурира от нея. Могат да се получават системни обновления през подсистемата за централизирано управление и да се обменят аларми и известия. **Източник:** FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 21, 279 **Източник:** CENTRAL MANAGEMENT ADMINISTRATION GUIDE RELEASE 8.7 Страници: 430
REQ.349.	Решението трябва да може да анализира файловете в локален sandbox, както и да може да изпраща файловете за анализ към външен sandbox, когато устройството е претоварено.	Решението може да анализира файловете в локален sandbox, както и може да изпраща файловете за анализ към външен sandbox, когато устройството е претоварено. **Източник:** FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3
REQ.350.	Решението трябва да разполага с IPMI интерфейс.	Решението разполага с IPMI интерфейс. Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 34
REQ.351.	Решението трябва да поддържа AAA протокол за контрол на потребителския достъп.	Решението поддържа AAA протокол за контрол на потребителския достъп.

		Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 119
REQ.352.	Решението трябва да разполага с вградени функции за филтриране на IP адреси, за да се защити интерфейса за управление от нежелан достъп.	Решението разполага с вградени функции за филтриране на IP адреси, за да се защити интерфейса за управление от нежелан достъп. Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 162
REQ.353.	Решението трябва да позволява определянето на използваните ресурси за sandbox анализ, за да се избегне претоварване на системата.	Решението позволява определянето на използваните ресурси за sandbox анализ, за да се избегне претоварване на системата. Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 225
REQ.354.	Решението трябва да поддържа наблюдение на показатели чрез SNMP.	Решението поддържа наблюдение на показатели чрез SNMP. Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3
REQ.355.	Решението трябва да предоставя функции за защитено изтриване на съхранени данни.	Решението предоставя функции за защитено изтриване на съхранени данни. Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 274
REQ.356.	Решението трябва да може да използва поне 190 виртуални машини за sandbox анализ по едно и също време.	Решението може да използва поне 190 виртуални машини за sandbox анализ по едно и също време. Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3

REQ.357.	Решението трябва да може да извършва автоматичен анализ на поне 60000 потенциално зловредни обекта на ден.	Решението може да извършва автоматичен анализ на 70000 потенциално зловредни обекта на ден. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/file/ds-file-protect.pdf
REQ.358.	Решението трябва да може да докладва за опитите за мрежово свързване на анализираните обекти във виртуалните машини.	Решението може да докладва за опитите за мрежово свързване на анализираните обекти във виртуалните машини. 
REQ.359.	Решението да може да извършва следствен анализ на откритите зловредни файлове и да може да предоставя копие на бинарния им (двоичен) код, както и PCAP файл с опитите им за мрежови свързвания, заедно с всички посетени URL адреси.	Решението да извършва следствен анализ на откритите зловредни файлове и може да предоставя копие на бинарния им (двоичен) код, както и PCAP файл с опитите им за мрежови свързвания, заедно с всички посетени URL адреси. **Източник:** FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 **Страници:** 169

REQ.360.	Решението трябва да може да извършва динамичен анализ за зловреден код, да може да се обновява и да може да му се предоставя нова информация за заплахи, дори в offline режим, без да има връзка с Интернет.	Решението може да извършва динамичен анализ за зловреден код, може да се обновява и може да му се предоставя нова информация за заплахи, дори в offline режим, без да има връзка с Интернет. Източник: DTI UPDATE PORTAL USER GUIDE RELEASE 1.4.1 Източник: OLP_UG_1.4.1_en.pdf Страници: 22
REQ.361.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението трябва да използва собствен, специално изграден хипервайзор.	Решението не използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението използва собствен, специално изграден хипервайзор. Източник: Thinking outside the box - fireeye-outside-sandbox.pdf Страници: 8
REQ.362.	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques).	Решението може да се справя с техники за избягване от засичане (evasion techniques). Източник: Thinking outside the box - fireeye-outside-sandbox.pdf Източник: fireeye-hot-knives-through-butter.pdf
REQ.363.	Решението трябва да разполага с графичен интерфейс, където да се изобразяват пълните детайли от извършения анализ на зловреден код.	Решението разполага с графичен интерфейс, където се изобразяват пълните детайли от извършения анализ на зловреден код. Източник: FILE SECURITY USER GUIDE RELEASE 8.3 Страници: 155

REQ.364.	Решението трябва да позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите трябва да могат да променят поне следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, използван Outlook акаунт, използвани език и часова зона.	Решението позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите могат да променят следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, използван Outlook акаунт, използвани език и часова зона.
REQ.365.	Решението трябва да може да тества и засича зловреден код в различни операционни системи на виртуалните машини за sandbox анализ, с различни версии на service pack, като да се поддържат както x64, така и x86 архитектури, под Windows и под Mac.	Решението може да тества и засича зловреден код в различни операционни системи на виртуалните машини за sandbox анализ, с различни версии на service pack, като се поддържат както x64, така и x86 архитектури, под Windows и под Mac. Източник: GI_RN_17.0112_en.pdf Страници: 6

REQ.366.	Решението трябва да може да извършва детайлен анализ и да открива зловреден код в следните файлови формати (минимално): изпълними .exe файлове, JAVA, PDF, MS Office документи, често срещани мултимедийни файлови формати като JPEG, QuickTime, MP3, архиви тип ZIP/RAR/7ZIP/TNEF, 3gp, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm.	Решението може да извършва детайлен анализ и открива зловреден код в следните файлови формати: изпълними .exe файлове, JAVA, PDF, MS Office документи, често срещани мултимедийни файлови формати като JPEG, QuickTime, MP3, архиви тип ZIP/RAR/7ZIP/TNEF, 3gp, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/file/ds-file-protect.pdf WIN10 x64

WIN XP

		OSX
REQ.367.	Решението трябва да позволява на администраторите да посочат кои приложения във виртуалните машини за анализ да стартират кои файлови типове.	Решението позволява на администраторите да посочат кои приложения във виртуалните машини за анализ да стартират кои файлови типове. Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 136
REQ.368.	Решението трябва да може да извършва цялостен анализ локално, без да е необходимо да излиза информация извън структурите на организацията.	Решението може да извършва цялостен анализ локално, без да е необходимо да излиза информация извън структурите на организацията. Източник: DTI UPDATE PORTAL USER GUIDE RELEASE 1.4.1 Източник: OLP_UG_1.4.1_en.pdf Страници: 22
REQ.369.	Решението трябва да поддържа LDAP или RADIUS методи за вписване на потребителите (минимално).	Решението поддържа LDAP и RADIUS методи за вписване на потребителите. Източник: SYSTEM SECURITY SYSTEM SECURITY GUIDE RELEASE 2019.4 Страници: 61-67

REQ.370.	Решението трябва да разполага с команден и с графичен интерфейс (достъпен през стандартен уеб-браузър) за централизирано управление.	Решението разполага с команден и с графичен интерфейс (достъпен през стандартен уеб-браузър) за централизирано управление. Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 25-31
REQ.371.	Решението трябва да може да работи в следните режими (за анализиране на файлове): • Сканиране по ръчни заявки (on-demand, с възможност и за анализ на отделни файлове) • Продължително сканиране на посочени файлови хранилища.	Решението може да работи в следните режими (за анализиране на файлове): • Сканиране по ръчни заявки (on-demand, с възможност и за анализ на отделни файлове) • Продължително сканиране на посочени файлови хранилища. Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 132, 138
REQ.372.	Решението трябва да позволява избирането на различни локации за преместване на файлове след анализ според това дали са със статус на „добър", „неизвестен" или „лош".	Решението позволява избирането на различни локации за преместване на файлове след анализ според това дали са със статус на „добър", „неизвестен" или „лош". Източник: FILE PROTECT SYSTEM ADMINISTRATION GUIDE RELEASE 8.3 Страници: 122
Хардуерни изисквания – 1 брой		**Предложение: 1 брой хардуерно устройство с вграден софтуер FireEye HW-6500 FX с включена 5-годишна поддръжка**
REQ.373.	Устройството да е с максимална големина 2RU	Устройството е с големина 2RU https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/file/ds-file-protec

REQ.374.	Устройството да разполага с поне 2TB за съхранение на данни	Устройството разполага с 4 x 2TB за съхранение на данни https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/file/ds-file-protect.pdf
REQ.375.	Устройството да разполага минимално със следните портове за свързване с мрежата: 4x 1GigE BaseT	Устройството разполага със следните портове за свързване с мрежата: 4x 1GigE BaseT https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/file/ds-file-protect.pdf
REQ.376.	Допълнителни портове: сериен порт, 4x Type A USB, IPMI	Устройството разполага със следните допълнителни портове: сериен порт, 4x Type A USB, IPMI https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/file/ds-file-protect.pdf
REQ.377.	Резервирано захранване – 1+1	Устройството разполага с резервирано захранване – 1+1 https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/file/ds-file-protect.pdf
REQ.378.	Устройството да може да анализира минимално 60000 файла на ден.	Устройството може да анализира 70000 файла на ден. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/file/ds-file-protect.pdf
REQ.379.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.	Устройството работи в изолиран режим, без Интернет свързаност. Устройството не изпраща данни към производителя за засечените заплахи в организацията. Източник: DTI UPDATE PORTAL USER GUIDE RELEASE 1.4.1

		Източник: OLP_UG_1.4.1_en.pdf Страници: 22
Гаранция и поддръжка:		**Предлагана гаранция и поддръжка от производителя:**
REQ.380.	Срок на хардуерната гаранция - минимум 5 (пет) години.	Срокът на хардуерната гаранция е 5 (пет) години.
REQ.381.	Срок на техническа поддържка – минимум 5 (пет) години.	Срокът на техническа поддръжка е 5 (пет) години.
REQ.382.	Получаване на нови версии на софтуера - минимум 5 (пет) години.	Новите версии на софтуера ще се получават 5 (пет) години.
REQ.383.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.	Обновяването на дефиниции и сигнатури е 5 (пет) години.

1.4.8. Подсистема за улавяне на мрежови пакети, разследвания и централизиран анализ и визуализация

Изискано от Възложителя		**Предложено от участника**
А.		**Б.**
Общи изисквания		
REQ.384.	Тип решение: • 1 брой хардуер за улавяне на мрежови пакети, с вграден софтуер и 5-годишна поддръжка; • 1 брой хардуер за разследвания и централизиран анализ и визуализация, с вграден софтуер и 5-годишна поддръжка;	Предлаганата подсистема за улавяне на мрежови пакети, разследвания и централизиран анализ и визуализация включва: **1 брой хардуерно устройство с вграден софтуер FireEye HW 2060ESS96 PX с включена 5-годишна поддръжка за улавяне на мрежови пакети; 1 брой хардуерно устройство с вграден софтуер FireEye HW 2100HN48 IA с включена 5-годишна поддръжка за централизиран анализ и визуализация;**

REQ.385.	Решението трябва да има пълна видимост над мрежовия трафик, чрез високоскоростно улавяне на мрежови пакети и анализ при мрежова производителност от 1800 Mbps за 4 интерфейса на ниво gateway. Решението трябва да може да се поставя в TAP/SPAN режим на работа, като да може да получава мрежовите данни след SSL декриптиране от настоящо решение за SSL декриптиране на организацията от трети производител (да има възможност за интеграция).	Решението има пълна видимост над мрежовия трафик, чрез високоскоростно улавяне на мрежови пакети и анализ при мрежова производителност от 2 Gbps за 4 интерфейса на ниво gateway. Решението може да се поставя в TAP/SPAN режим на работа, като може да получава мрежовите данни след SSL декриптиране от настоящо решение за SSL декриптиране на организацията от трети производител (има възможност за интеграция). https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/entfor/fireeye-network-forensics-platform.pdf
REQ.386.	Решението да има възможност за изключително бързо (в реално време) записване и индексиране на мрежови трафик.	Решението има възможност за изключително бързо (в реално време) записване и индексиране на мрежови трафик. Източник: PX SERIES USER GUIDE RELEASE 5.1.1 Страници: 13
REQ.387.	Решението трябва да може да улавя, търси и анализира информацията от мрежовите пакети и сесии.	Решението може да улавя, търси и анализира информацията от мрежовите пакети и сесии. Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 Страници: 11
REQ.388.	Решението трябва да може да чете и записва пакети в PCAP формат.	Решението може да чете и записва пакети в PCAP формат. Източник: PX SERIES USER GUIDE RELEASE 5.1.1 Страници: 15
REQ.389.	Решението трябва да позволява извършването на филтрирани търсения, използвайки често срещани	Решението позволява извършването на филтрирани търсения, използвайки често срещани

	стойности за адрес, приложение, протокол, VLAN, MPLS, метаданни от мрежовата връзка.	стойности за адрес, приложение, протокол, VLAN, MPLS, метаданни от мрежовата връзка. Източник: PX SERIES USER GUIDE RELEASE 5.1.1 Страници: 26
REQ.390.	Решението трябва да поддържа интеграция с подсистема за засичане, защита и разследване на непознати заплахи на ниво крайна точка, за да може да получава информация за вътрешно наблюдаваните IP адреси от крайните точки и за да може да извлича потребителските имена, асоциирани с дадено име на хост.	Решението поддържа интеграция с подсистема за засичане, защита и разследване на непознати заплахи на ниво крайна точка, за да получава информация за вътрешно наблюдаваните IP адреси от крайните точки и за да извлича потребителските имена, асоциирани с дадено име на хост. Източник: IA SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 1.5 Страници: 108, 112
REQ.391.	Решението трябва да може да анализира мрежови сесии и да извлича файлове от тях.	Решението може да анализира мрежови сесии и да извлича файлове от тях. Източник: PX SERIES USER GUIDE RELEASE 5.1.1 Страници: 37
REQ.392.	Решението трябва да позволява на анализаторите да търсят в мрежовия трафик ключови думи и регулярни изрази на ниво приложен слой.	Решението позволява на анализаторите да търсят в мрежовия трафик ключови думи и регулярни изрази на ниво приложен слой. https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/entfor/fireeye-network-forensics-platform.pdf
REQ.393.	Решението трябва да поддържа сложни заявки, използващи булева логика.	Решението поддържа сложни заявки, използващи булева логика. Източник: IA SERIES USER GUIDE RELEASE 1.5 Страници: 83

REQ.394.	Решението трябва да може да се интегрира и изпраща извлечени файлове от мрежови сесии директно към подсистема (лаборатория) за динамичен анализ на зловреден код.	Решението може да се интегрира и изпраща извлечени файлове от мрежови сесии директно към подсистема (лаборатория) за динамичен анализ на зловреден код. Източник: IA SERIES USER GUIDE RELEASE 1.5 Страници: 165
REQ.395.	Решението трябва да може да реконструира уеб-страници и email съобщения от уловения мрежови трафик. Също така, трябва да може да реконструира POP3/IMAP/FTP/SMB.	Решението може да реконструира уеб-страници и email съобщения от уловения мрежови трафик. Решението може да реконструира POP3/IMAP/FTP/SMB. Източник: IA SERIES USER GUIDE RELEASE 1.5 Страници: 123, 125, 155
REQ.396.	Решението трябва да може да извлича данни от много големи файлове с мрежови трафик, до 1 гигабайт.	Решението може да извлича данни от много големи файлове с мрежови трафик, до 1 гигабайт. Източник: IA SERIES USER GUIDE RELEASE 1.5 Страници: 155
REQ.397.	Решението трябва да може да кодира/декодира следните формати от данни: Base64, gzip, HEX, HEXDUMP, JSON, URL, XOR.	Решението може да кодира/декодира следните формати от данни: Base64, gzip, HEX, HEXDUMP, JSON, URL, XOR. Източник: IA SERIES USER GUIDE RELEASE 1.5 Страници: 127
REQ.398.	Решението трябва да позволява определянето на собствени правила, на базата на които да се улавя и съхранява мрежовия трафик за по-нататъшен анализ.	Решението позволява определянето на собствени правила, на базата на които се улавя и съхранява мрежовия трафик за по-нататъшен анализ. Източник: PX SERIES USER GUIDE RELEASE 5.1.1 Страници: 64

REQ.399.	Решението трябва да може да анализира в детайли следните протоколи: DCE-RPC, IPv6, SMB, DHCP, IRC, SMB2, DNS, MODBUS, SMTP, ERSPAN, MPLS, SSL, FTP, MSN, SSH, GRE, POP3, TCP, HTTP, PPP, TEREDO, ICMPv4, RDP, TLS, ICMPv6, RTSP, UDP, IMAP, SCTP, VLAN, IPv4, SIP, IPFIX, NETFLOWv5, NETFLOWv9.	Решението може да анализира в детайли следните протоколи: DCE-RPC, IPv6, SMB, DHCP, IRC, SMB2, DNS, MODBUS, SMTP, ERSPAN, MPLS, SSL, FTP, MSN, SSH, GRE, POP3, TCP, HTTP, PPP, TEREDO, ICMPv4, RDP, TLS, ICMPv6, RTSP, UDP, IMAP, SCTP, VLAN, IPv4, SIP, IPFIX, NETFLOWv5, NETFLOWv9. Източник: PX SERIES USER GUIDE RELEASE 5.1.1 Страници: 83
REQ.400.	Решението трябва да позволява търсене в индексираните метаданни на следните протоколи: HTTP, DNS, SMTP, POP3, IMAP, SSL, TLS, FTP, SSH и MODBUS.	Решението позволява търсене в индексираните метаданни на следните протоколи: HTTP, DNS, SMTP, POP3, IMAP, SSL, TLS, FTP, SSH и MODBUS Източник: IA SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 1.5 Страници: 12
REQ.401.	Решението трябва да може да разпознава минимално следните приложения: AFP, Aimini, Amazon, Apple, AppleiCloud, AppleiTunes, AppleJuice, Armagetron, AVI, Ayiya, BattleField, BGP, BitTorrent, CiscoSkinny, CiscoVPN, Citrix, Citrix_Online, CNN, Collectd, Corba, Crossfire, DCE_RPC, DHCP, DHCPV6, DirectConnect, Direct_Download_Link, DNS, Dofus, DropBox, eBay, eDonkey, EGP, EPP, Facebook, FacebookChat, FastTrack, Fiesta, Filetopia, Flash, Florensia, FTP, FTP_CONTROL, FTP_DATA, GMail, Gnutella, Google, GoogleMaps, GRE, GrooveShark, GTP, Guildwars, H323, HalfLife2, HTTP, HTTP_Application_ActiveSync, HTTP_APPLICATION_VEOHTV, HTTP_Connect, HTTP_Proxy, IAX, IceCast, ICMP, ICMPV6, IGMP, IMAP, IMAPS, iMESH, IPP, IPsec, IP_in_IP, IRC, Jabber, Kerberos, Kontiki, LastFM, LDAP, LLMNR,	Решението може да разпознава следните приложения: AFP, Aimini, Amazon, Apple, AppleiCloud, AppleiTunes, AppleJuice, Armagetron, AVI, Ayiya, BattleField, BGP, BitTorrent, CiscoSkinny, CiscoVPN, Citrix, Citrix_Online, CNN, Collectd, Corba, Crossfire, DCE_RPC, DHCP, DHCPV6, DirectConnect, Direct_Download_Link, DNS, Dofus, DropBox, eBay, eDonkey, EGP, EPP, Facebook, FacebookChat, FastTrack, Fiesta, Filetopia, Flash, Florensia, FTP, FTP_CONTROL, FTP_DATA, GMail, Gnutella, Google, GoogleMaps, GRE, GrooveShark, GTP, Guildwars, H323, HalfLife2, HTTP, HTTP_Application_ActiveSync, HTTP_APPLICATION_VEOHTV, HTTP_Connect, HTTP_Proxy, IAX, IceCast, ICMP, ICMPV6, IGMP, IMAP, IMAPS, iMESH, IPP, IPsec, IP_in_IP, IRC, Jabber, Kerberos, Kontiki, LastFM, LDAP, LLMNR, LotusNotes, MapleStory, MDNS, Meebo, Megaco, MGCP, MMS, Move,

	LotusNotes, MapleStory, MDNS, Meebo, Megaco, MGCP, MMS, Move, MPEG, MSN, MsSQL, MySQL, NetBIOS, NetFlix, NFS, NOE, NTP, OggVorbis, OpenFT, OpenVPN, Oracle, Oscar, OSPF, Pandora, Pando_Media_Booster, PcAnywhere, POP, POP3, POPS, PostgreSQL, PPLive, PPStream, PPTP, QQ, QQLive, Quake, QuickTime, Radius, RDP, RealMedia, Redis, RemoteScan, RSYNC, RTCP, RTMP, RTP, RTSP, SAP, SCTP, sFlow, ShoutCast, SIP, SkyFile_PostPaid, SkyFile_PrePaid, SkyFile_Rudics, Skype, SMB, SMTP, SMTPS, SNMP, SOCKS4, SOCKS5, Socrates, Sopcast, Soulseek, Spotify, SSDP, SSH, SSL, SSL_No_Cert, Stealthnet, Steam, STUN, Syslog, TDS, TeamSpeak, TeamViewer, Telegram, Telnet, TFTP, Thunder, TOR, TruPhone, Tuenti, Tvants, TVUplayer, Twitter, UbuntuONE, Unencryped_Jabber, Unknown, UPnP, Usenet, VEOHTV, VHUA, Viber, VMware, VNC, VRRP, Warcraft3, Webex, WebM, Whois-DAS, WhatsApp, Wikipedia, WindowsMedia, WindowsUpdate, WinMX, WorldOfKungFu,WorldOfWarcraft, Xbox, XDMCP, Yahoo, YouTube, Zattoo, ZeroMQ.	MPEG, MSN, MsSQL, MySQL, NetBIOS, NetFlix, NFS, NOE, NTP, OggVorbis, OpenFT, OpenVPN, Oracle, Oscar, OSPF, Pandora, Pando_Media_Booster, PcAnywhere, POP, POP3, POPS, PostgreSQL, PPLive, PPStream, PPTP, QQ, QQLive, Quake, QuickTime, Radius, RDP, RealMedia, Redis, RemoteScan, RSYNC, RTCP, RTMP, RTP, RTSP, SAP, SCTP, sFlow, ShoutCast, SIP, SkyFile_PostPaid, SkyFile_PrePaid, SkyFile_Rudics, Skype, SMB, SMTP, SMTPS, SNMP, SOCKS4, SOCKS5, Socrates, Sopcast, Soulseek, Spotify, SSDP, SSH, SSL, SSL_No_Cert, Stealthnet, Steam, STUN, Syslog, TDS, TeamSpeak, TeamViewer, Telegram, Telnet, TFTP, Thunder, TOR, TruPhone, Tuenti, Tvants, TVUplayer, Twitter, UbuntuONE, Unencryped_Jabber, Unknown, UPnP, Usenet, VEOHTV, VHUA, Viber, VMware, VNC, VRRP, Warcraft3, Webex, WebM, Whois-DAS, WhatsApp, Wikipedia, WindowsMedia, WindowsUpdate, WinMX, WorldOfKungFu, WorldOfWarcraft, Xbox, XDMCP, Yahoo, YouTube, Zattoo, ZeroMQ. Източник: PX SERIES USER GUIDE RELEASE 5.1.1 Страници: 93
REQ.402.	Решението трябва да може да анализира следните видове мрежови трафик: използващ IPv4 протокол; използващ IPv6 протокол.	Решението може да анализира следните видове мрежови трафик: използващ IPv4 протокол; използващ IPv6 протокол. Източник: PX SERIES USER GUIDE RELEASE 5.1.1 Страници: 83
REQ.403.	Решението трябва да предоставя на администраторите разбираем и с възможност за модифициране интерфейс със списъци, графики и географски карти.	Решението предоставя на администраторите разбираем и с възможност за модифициране интерфейс със списъци, графики и географски карти. Източник: IA SERIES USER GUIDE RELEASE 1.5

		Страници: 21, 39
REQ.404.	Решението трябва да позволява на администраторите лесно и бързо да извършват „reverse DNS lookup“ и „whois“ проверки директно от уеб интерфейса.	Решението позволява на администраторите лесно и бързо да извършват „reverse DNS lookup“ и „whois“ проверки директно от уеб интерфейса. Източник: IA SERIES USER GUIDE RELEASE 1.5 Страници: 121
REQ.405.	Решението трябва да позволява на анализаторите да преглеждат данните на ниво мрежова връзка, пакет и payload.	Решението позволява на анализаторите да преглеждат данните на ниво мрежова връзка, пакет и payload. Източник: IA SERIES USER GUIDE RELEASE 1.5 Страници: 121
REQ.406.	Решението трябва да може да приема аларми от другите подсистеми за киберсигурност.	Решението може да приема аларми от другите подсистеми за киберсигурност. Източник: IA SERIES USER GUIDE RELEASE 1.5 Страници: 25, 145
REQ.407.	Решението за улавяне на мрежови пакети трябва да използва „full disk encryption“ метод за криптиране на събраните данни и метаданни.	Решението за улавяне на мрежови пакети използва „full disk encryption“ метод за криптиране на събраните данни и метаданни. Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 Страници: 11
REQ.408.	Решението за улавяне на мрежови пакети трябва да може да се интегрира с SAS RAID или с HBA контролер, за да се гарантира непрекъснат процес на събирането на мрежови пакети.	Решението за улавяне на мрежови пакети може да се интегрира с SAS RAID или с HBA контролер, за да се гарантира непрекъснат процес на събирането на мрежови пакети. Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 Страници: 11

REQ.409.	Решението трябва да разполага с IPMI интерфейс.	Решението разполага с IPMI интерфейс. Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 Страници: 64 Източник: IA SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 1.5 Страници: 30
REQ.410.	Решението трябва да поддържа автентикация на потребителите с протоколи PAM/LDAP/RADIUS/TACACS+. Да се поддържа ролево-базирано управление, потребителите да могат да имат различни роли (администратор, анализатор, т.н.)	Решението поддържа автентикация на потребителите с протоколи PAM/LDAP/RADIUS/TACACS+. Решението поддържа ролево-базирано управление, като потребителите могат да имат различни роли (администратор, анализатор, т.н.) Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 Страници: 47, 49 Източник: IA SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 1.5 Страници: 116
REQ.411.	Решението трябва да може да засича извличане на данни извън организацията.	Решението може да засича извличане на данни извън организацията. Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 Страници: 60
REQ.412.	Решението трябва да поддържа Suricata правила за дефиниции/алармиране.	Решението поддържа Suricata правила за дефиниции/алармиране. Източник: IA SERIES USER GUIDE RELEASE 1.5

		Страници: 63 Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 Страници: 61
REQ.413.	Решението трябва да позволява задаването на правила за филтриране на мрежовия трафик. Правилата са необходими за намаляване на обема анализиран трафик. Тези правила трябва да са наложени директно на хардуерните интерфейси за улавяне на трафика, преди да затормозят централният процесор на системата. Да може да се филтрира минимално на база следните параметри: src IP, src port, dst IP, dst port.	Решението позволява задаването на правила за филтриране на мрежовия трафик, за намаляване на обема анализиран трафик. Тези правила са наложени директно на хардуерните интерфейси за улавяне на трафика, преди да затормозят централният процесор на системата. Може да се филтрира на база следните параметри: src IP, src port, dst IP, dst port. Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 Страници: 67
REQ.414.	Решението трябва да може да извлича метаданни от уловения мрежови трафик през HTTP.	Решението може да извлича метаданни от уловения мрежови трафик през HTTP. Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 Страници: 69
REQ.415.	Решението трябва да може да индексира в реално време уловените мрежови пакети, използвайки маркери за време и атрибутите на мрежовите свързвания. Да могат да се извличат индекса на потока от данни и метаданните на мрежовата връзка в JSON формат.	Решението може да индексира в реално време уловените мрежови пакети, използвайки маркери за време и атрибутите на мрежовите свързвания. Могат да се извличат индекса на потока от данни и метаданните на мрежовата връзка в JSON формат. Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 Страници: 108

REQ.416.	Решението трябва да предоставя информация за собствените си процеси и за складираните данни, за да може да се планира капацитета в бъдеще.	Решението предоставя информация за собствените си процеси и за складираните данни, за да може да се планира капацитета в бъдеще. Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 Страници: 82 Източник: IA SERIES USER GUIDE RELEASE 1.5 Страници: 169
REQ.417.	Решението трябва да позволява да му се наблюдават параметрите по производителността чрез SNMP.	Решението позволява да му се наблюдават параметрите по производителността чрез SNMP. Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 Страници: 86 Източник: IA SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 1.5 Страници: 34
REQ.418.	Решението трябва да предоставя възможност за сигурно изтриване на данните от дисковото му пространство, чрез презаписване (overwrite) на данните множество пъти.	Решението предоставя възможност за сигурно изтриване на данните от дисковото му пространство, чрез презаписване (overwrite) на данните множество пъти. Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 Страници: 98 Източник: IA SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 1.5 Страници: 126

REQ.419.	Решението трябва да може да се интегрира с източници на информация за заплахи.	Решението може да се интегрира с източници на информация за заплахи. **Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1** **Страници: 106** **Източник: IA SERIES USER GUIDE RELEASE 1.5** Страници: 73
REQ.420.	Решението трябва да позволява добавянето на множество нови индикатори за компроментиране чрез формати STIX и OpenIOC.	Решението позволява добавянето на множество нови индикатори за компроментиране чрез формати STIX и OpenIOC. **Източник: IA SERIES USER GUIDE RELEASE 1.5** **Страници: 73**
REQ.421.	Решението трябва да позволява определяне на времеви интервал за автоматично търсене за индикатори за компроментиране в събраните метаданни и да може да вдига аларми за тях.	Решението позволява определяне на времеви интервал за автоматично търсене за индикатори за компроментиране в събраните метаданни и може да вдига аларми за тях. Източник: IA SERIES USER GUIDE RELEASE 1.5
REQ.422.	Решението трябва да поддържа изпозлването на reverse SSH и HTTPS тунели, за да може да се интегрира със системи от външна мрежа.	Решението поддържа изпозлването на reverse SSH и HTTPS тунели, за да може да се интегрира със системи от външна мрежа. Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 **Страници: 114**
REQ.423.	Решението трябва да поддържа автентикация с използване на smart карти.	Решението поддържа автентикация с използване на smart карти.

		Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 Страници: 119 Източник: IA SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 1.5 Страници: 130
REQ.424.	Решението трябва да предоставя достъп за търсене в съхранените метаданни.	Решението предоставя достъп за търсене в съхранените метаданни. Източник: IA SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 1.5 Страници: 121
REQ.425.	Решението трябва да може да се интегрира и да приема метаданни на слой 7 от подсистема за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво, както и да може да изисква уловени пакети по конкретно събитие, за което е вдигната аларма.	Решението може да се интегрира и да приема метаданни на слой 7 от подсистема за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво, както и може да изисква уловени пакети по конкретно събитие, за което е вдигната аларма. Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 Страници: 121
REQ.426.	Решението трябва да разполага с API интерфейс.	Решението разполага с API интерфейс Източник: IA SERIES API REFERENCE RELEASE 1.5 Източник: PX SERIES API REFERENCE RELEASE 5.1.1
REQ.427.	Решението за улавяне на мрежови пакети трябва да е изградено с подсилена откъм сигурност, заключена операционна система.	Решението за улавяне на мрежови пакети е изградено с подсилена откъм сигурност, заключена операционна система. Източник: PX SERIES USER GUIDE RELEASE 5.1.1

		Страници: 13
REQ.428.	Решението за улавяне на мрежови пакети трябва да може да съхранява събраните PCAP данни и метаданни за поне 14 дена, при събиране на данни 8 часа на ден при количество трафик от 1 Gbps.	Решението за улавяне на мрежови пакети може да съхранява събраните PCAP данни и метаданни за поне 14 дена, при събиране на данни 8 часа на ден при количество трафик от 1 Gbps. Източник: PX SERIES SYSTEM ADMINISTRATION GUIDE RELEASE 5.1.1 https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/entfor/fireeye-network-forensics-platform.pdf
Хардуерни изисквания за хардуерно устройство за улавяне на мрежови пакети		**Предложение: 1 брой хардуерно устройство с вграден софтуер FireEye HW 2060ESS96 PX с включена 5-годишна поддръжка**
REQ.429.	Устройството да е с максимална големина 2U	Устройството е с големина 2U https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/entfor/fireeye-network-forensics-platform.pdf
REQ.430.	Устройството да разполага с поне 95TB за съхранение на данни, с възможност за разширяване на обема със скачено SAS дисково пространство	Устройството разполага с 96TB за съхранение на данни, с възможност за разширяване на обема със скачено SAS дисково пространство https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/entfor/fireeye-network-forensics-platform.pdf
REQ.431.	Устройството да разполага минимално със следните портове за свързване с мрежата: 4 x 10GE SFP+	Устройството разполага със следните портове за свързване с мрежата: 4 x 10GE SFP+ https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/entfor/fireeye-network-forensics-platform.pdf

REQ.432.	Допълнителни портове: 2 x 1GbE портове за управление	Устройството разполага със следните допълнителни портове: 2 x 1GbE портове за управление https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/entfor/fireeye-network-forensics-platform.pdf
REQ.433.	Резервирано захранване – 1+1	Устройството разполага с резервирано захранване – 1+1 https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/entfor/fireeye-network-forensics-platform.pdf
REQ.434.	Устройството да може да записва мрежови данни със скорост от 1800 Mbps	Устройството може да записва мрежови данни със скорост от 2 Gbps https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/entfor/fireeye-network-forensics-platform.pdf
Хардуерни изисквания за хардуерно устройство за разследвания и централизиран анализ и визуализация		**Предложение: 1 брой хардуерно устройство с вграден софтуер FireEye HW 2100HN48 IA с включена 5-годишна поддръжка**
REQ.435.	Устройството да е с максимална големина 2U	Устройството е с големина 2U https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/entfor/fireeye-network-forensics-platform.pdf
REQ.436.	Устройството да разполага с поне 45TB за съхранение на данни	Устройството разполага с 48TB за съхранение на данни https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/entfor/fireeye-network-forensics-platform.pdf

REQ.437.	Резервирано захранване – 1+1	Устройството разполага с резервирано захранване – 1+1 https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/entfor/fireeye-network-forensics-platform.pdf
Гаранция и поддръжка:		
REQ.438.	Срок на хардуерната гаранция - минимум 5 (пет) години.	Срокът на хардуерната гаранция е 5 (пет) години.
REQ.439.	Срок на техническа поддържка – минимум 5 (пет) години.	Срокът на техническа поддръжка е 5 (пет) години.
REQ.440.	Получаване на нови версии на софтуера - минимум 5 (пет) години.	Новите версии на софтуера ще се получават 5 (пет) години.
REQ.441.	Обновяване на дефиниции и сигнатури – минимум 5 (пет)години.	Обновяването на дефиниции и сигнатури е 5 (пет) години.

Забележка: а) *Навсякъде в техническата спецификация, където се съдържа посочване на конкретен модел, източник, процес, търговска марка, патент, тип, произход, стандарт или производство да се чете и разбира „или ЕКВИВАЛЕНТ". Участникът следва да докаже, че предлаганите решения удовлетворяват по еквивалентен начин изискванията, определени от техническата спецификация.*

б) *Оборудването, предмет на доставката, се състои от хардуер и софтуер, които трябва да съответстват или да надвишават в техническо отношение посочените минимални изисквания в Техническата спецификация и приложението към нея, относимо към настоящата обособена позиция.*

2. Изисквания към изпълнението на поръчката:

2.1. Декларираме, че оборудването, предмет на доставката, ще бъде фабрично ново, неупотребявано, включено е в актуалните продуктови листи на производителя, ще продължава да бъде включено към датата на сключване на договора за възлагане на обществената поръчка и не е спряно от производство.

2.2. Хардуерните компоненти на оборудването ще отговарят на всички стандарти в Република България относно ергономичност, пожарна безопасност, норми за безопасност и включване към електрическата мрежа.

2.3. Оборудването ще бъде доставено в пълно работно състояние, в оригиналната опаковка на производителя с ненарушена цялост, окомплектовано с всички необходими интерфейсни и захранващи кабели, в случай, че са различни от стандартни IEC C14 - IEC C13 или IEC C20 - IEC C19. Необходимата техническа документация, като потребителски, инсталационни, конфигурационни и др. ръководства ще се представят на електронен носител за всеки тип от предлаганите устройства.

2.4. При доставката на софтуер ще бъдат предоставени необходимите сертификати или други документи, удостоверяващи предоставеното право на ползване на софтуера.

3. Условия на доставка

3.1. Запознати сме, че доставката на оборудването ще се извършва въз основа на писмена заявка, отправена чрез адреса за кореспонденция на хартиен носител или по електронна поща, подписана с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис на възложителя или упълномощен негов представител, съгласно клаузите на договора за обществена поръчка.

3.2. Приемането и предаването на изпълнението ще се осъществява въз основа на изискванията на договора за обществена поръчка.

4. Условия на гаранционно обслужване

4.1. Гарантираме за срока, посочен в т. 5.2., пълната функционална годност на доставеното оборудване съгласно предписанията на производителя, изискванията на договора за обществена поръчка по обособената позиция, за която предоставяме настоящето Техническо предложение и приложенията към него.

4.2. В рамките на срока по посочен в т. 5.2. се задължаваме да отстраняваме за наша сметка всички повреди и/или несъответствия на оборудването, съответно подменя дефектирали части, устройства, модули и/или компоненти с нови съгласно предписанията на производителя, изискванията на договора за обществена поръчка по обособената позиция, за която предоставяме настоящето Техническо предложение и приложенията към него. В гаранционното обслужване се включва замяна на част (компонент) със скрити недостатъци с нова или на цялото устройство с ново, ако недостатъкът го прави негодно за използване по предназначението му, както и всички разходи по замяната.

4.3. Редът за отстраняване на констатиран дефект и/или несъотвествие в срока на гаранционно обслужване е описан в договора за обществена поръчка по обособената позиция, за която предоставяме настоящето Техническо предложение.

5. Срок на изпълнение

5.1. Задължаваме се да извършим доставка на оборудването в срок до 30 календарни дни, считано от датата на получаване на писмена заявка по чл. 1, ал. 2 от проекта на договор за обществена поръчка.

***Забележка**: Участникът следва да предложи в офертата си срок за извършване на доставката, който не може да бъде по-дълъг от 80 календарни дни, считано от получаване на писмената заявка по чл. 1, ал. 2 от проекта на договор за обществена поръчка.*

5.2. Срокът на гаранционно обслужване е 5 години, считано от датата на приемо-предавателния протокол за доставка на оборудването.

***Забележка**: Участникът следва да предложи в офертата си срок за гаранционно обслужване, който следва да бъде минимум 5 (пет) години, считано от датата на подписване на двустранен приемо-предавателен протокол за приемане на доставката.*

6. Място на изпълнение

6.1. Потвърждаваме, че мястото на извършване на доставката е на територията на гр. София, като сме запознати, че ще бъде посочено в писмената заявка конкретния адрес на извършване на доставката.

6.2. Гаранционното обслужване ще се извършва спрямо местонахождението на доставеното и инсталирано оборудване.

7. Други изисквания

7.1. Декларираме, че сме надлежно упълномощени да извършваме доставка и гаранционно обслужване на предлаганото от нас комуникационно оборудване и изчислителна инфраструктура, необходими за обновяване на информационни и комуникационни системи на територията на Република България.

За удостоверяване на горното представяме ***Официално оторизационно писмо от производителя FireEye*** (моля, посочете описание на документа)

Забележка: *За удостоверяване на горното участникът следва да представи Официално оторизационно писмо (или еквивалентен документ) с актуална дата от производителя или от официален представител на производителя на предлаганото оборудване. Горепосоченият документ се представя в техническото предложение на участника.*

В случаите на представяне от участника на оторизационно писмо (или еквивалентен документ) от официален представител на производителя, в офертата се прилага и

оторизационно писмо, издадено от производителя (или еквивалентен документ), с което се упълномощава официалния представител на производителя за доставка и гаранционно обслужване на предлаганото оборудване.

7.2. Прилагаме **Общи условия за гаранционно обслужване на продуктите, предмет на обществената поръчка от производителя FireEye – Приложение №1 към Техническото предложение; Общи условия за извършване на доставки и гаранционна поддръжка от фирма КОМПЮТЪР 2000 България ЕООД – Приложение №2 към Техническото предложение,** както и **продуктови брошури за продуктите, предмет на обществената поръчка**.

Дата на подписване:	**10/ 07 / 2020**
Подпис и печат:	**.....**
Име и фамилия	**Анелия Костадинова**
Длъжност	**Управител**
Наименование на участника	**„КОМПЮТЪР 2000 България“ ЕООД**

Stiliyana Mahaldjiiska
L&S TRANSLATION OFFICE

Превод от

Продуктова брошура

FireEye Endpoint Security Брошура със спецификации

Общо представяне
FireEye Endpoint Security съчетава най-доброто от предишните продукти за сигурност на крайна точка и го подобрява с технологията, експертизата и информацията на FireEye за защита от днешните кибер атаки.

Опции за внедряване
Endpoint Security може да се използва като хардуерно устройство, което защитава до 100 000 крайни точки, виртуално устройство или чрез облак. Физическото устройство HX4502 може да се използва както за основната мрежа, така и за DMZ внедряване - единствената разлика е в лицензирането на всяко устройство; хардуерът е идентичен.

Таблица 1. Спецификации на виртуалното устройство.

Модел на лицензa	HX2500V (D)	HX2502V	HX4500V (D)	HX4502V
Максимален брой поддържани крайни точки	15,000	15,000	100,000	100,000
CPU	4 ядра	4 ядра	8 ядра	8 ядра
Памет	16 GB RAM	16 GB RAM	64 GB RAM	64 GB RAM
Диск	512 GB Диск	1200 GB Диск	1200 Диск	3600 GB Диск
Виртуални NICs	2 vmxnet3 интерфейси	2 vmxnet3 интерфейси	2 vmxnet3 интерфейси	2 vmxnet3 интерфейси

Изисквания на виртуалното устройство
Виртуалните устройства на Endpoint Security изискват следните VMware ресурси:

- VMware ESXi хост версия 6.0 или по-нова версия. По-старите версии на ESXi не се поддържат
- VMware vSphere Client
- VMXNET 3 мрежови софтуери
- Стандартен виртуален превключвател, създаден за портовете за наблюдение на виртуалните устройства, и прикачен към физически мрежов адаптер на ESXi сървъра.
- VMware VCenter Server (препоръчително). Когато използвате vSphere Client за добавяне на виртуални устройства към vCenter сървър, съветникът за инсталиране Deploy OVG Template предоставя лесен начин за въвеждане на код за активиране. В противен случай трябва да го въведете в конзолата на виртуалното устройство, тъй като не можете да го поставите в тази конзола.

0002445

ЕТ „Л и С - Стилияна Махалджийска“
Офис „Изток“: 1113 София, ул. Жолио Кюри 46Б, тел./факс: 02 963 44 04
Офис „Младост 1“: 1784 София, бул. Йерусалим, бл. 54, офис 11, партер (в двора), тел./факс: 02 974 57 55
Офис „Бизнес парк София“: 1715 София, Бизнес парк София, сграда 8, вх. А - Б, тел.: 02 489 81 55
ЕТ „L&S - Stiliyana Mahaldjiiska“
Office „Istok“: 1113 Sofia Bulgaria, 46B, Fr. J. Curie Str., tel./fax: 02 963 44 04
Office „Mladost 1“: 1784 Sofia Bulgaria, 54, Yerusalim Blvd., Office 11, ground floor, tel./fax: 02 974 57 55
Office „Business Park Sofia“: 1715 Sofia Bulgaria, Business Park Sofia, building 8, ent. A-B, tel.: +359 2 489 81 55
office@variante.info
sliai@abv.bg
+359 888 875 932
www.variante.info

блица 2. Спецификации на физическото устройство.

ле на модела	HX4502 or HX4502-D
аксимален брой управлявани крайни чки	100,000
азмер на устройството	1U
PU описание	E3-1240 v5, 4c, 3.5GHz
рой CPU	1
писание на паметта	DDR4 ECC UDIMM 16GB, 2133MHz
рой DIMM	4
бщо памет (GB)	64
ортове за интерфейс на дънната латка	2x 1GigE BaseT, 1x IPMI, 2x USB2 (заден), 2x USB3 (заден), 1x DB9 Serial, 1x VGA
допълнителни модули	TPM 1.2 (9655 4.34)
допълнителни карти	LSI9341-4i, 2x 1GigE BaseT
ffective Storage Capacity	8TB
рой памет	4
апацитет за съхранение на устройсто	4TB
ид памет	HDD, 3.5", SAS3, 7.2krpm
дове RAID	RAID 10
азмери на шасито ШхДхВ inch (mm)	17.2in (437mm) x 25.6in (650mm) x 1.7in (43.2mm)
егло на шасито lbs (Kg)	30.0 lbs. (13.6Kg)
Доставен пакет ШхДхВ in (mm)	34.5in (880mm) x 23.5in (600mm) x 9.25in (180mm)
егло на доставения пакет lbs. (Kg)	41.0lbs. (18.6Kg)
Топлинно отделяне при максимална мощност BTU / Hr. (W)	836BTU / Hr (245W)
PSU	Redundant (1+1) 750 watt, 100 - 240 VAC 8.0 – 4.5A, 50-60 Hz IEC60320-C14 inlet, FRU
MTBF (Hrs.)	54,200
Съответствие с изискванията за безопасност	UL 60950-1-2014; CAN/; CSA C22.2 No. 60950-1-07; Am.1:2011+Am.2:2014; AS/NSZ 60950.1- 2011
EMC съответствие	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN55022 Class A; VCCI V-3 Class A; EN 55024; EN61000-3-2 Class A; EN 61000-3-3; CNS 13438 (2006) Class A; CISPR22 Class A; AS/NZS CISPR 22 Class A; KN 32; KN 35
Съответствие с изискванията за опазване на околната среда	RoHS; REACH; WEEE
Работна температура	32 ~ 95° F (0 ~ 35° C)
Работна относителна влажност	10 ~ 95% @ 40° C, без кондензация
Температура в изключен режим	-40 ~ 158° F (-40 ~ 70° C)
Относителна влажност в изключен режим	10 ~ 95% @ 60° C, без кондензация
Работна височина	5000 ft. (1524 m.)

За да научите повече за FireEye, посетете: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2019 FireEye, Inc. . FireEye е регистрирана търговска марка на FireEye, Inc. Всички други марки, продукти или услуги са или могат да бъдат търговски марки или марки на услуги на съответните им собственици.
EP EXT-DS-US-EN-000023-02

За FireEye, Inc.
FireEye е компания за интелигентна охрана. Работейки като безпроблемно, мащабируемо разширение на защитните операции на клиентите, FireEye предлага единна платформа, която съчетава иновативни технологии за сигурност, информация заплахи на национално ниво и световно призната консултация Mandiant®. С този подход FireEye елиминира сложността и тежестта на киберсигурността за организации, които се борят да се подготв предотвратяват и реагират на кибератаки.

FIREEYE

ЕТ "L&S - St. Mahaldjiiska" Sofia L&S София ЕТ "ЛиС - Ст. Мехалджийска"

Подписаната, [redacted], ЕГН: [redacted], Потвърждение №: 18ПР-1398/26.02.2018 г., удостоверявам верността на превода от английски на български език на приложения документ –, извършен от мен. Преводът се състои от 3 страници.

Подпис: [redacted]

L&S

[redacted]

[redacted]

[redacted]

[redacted]

FIREEYE™

DATA SHEET

FireEye Endpoint Security Specification Sheet

Overview

FireEye Endpoint Security combines the best of legacy endpoint security products, and enhances it with FireEye technology, expertise and intelligence to defend against today's cyber attacks.

Deployment options

Endpoint Security can be deployed as an on-premise hardware appliance that protects up to 100,000 endpoints, a virtual appliance, or through a cloud instance. The HX4502 physical appliance can be used for either core or DMZ deployment — the only difference is the license state of each device; the hardware is identical.

Table 1. Virtual appliance specifications.

License Model	HX2500V (D)	HX2502V	HX4500V (D)	HX4502V
Max Endpoints Supported	15,000	15,000	100,000	100,000
CPU	4 cores	4 cores	8 cores	8 cores
Memory	16 GB RAM	16 GB RAM	64 GB RAM	64 GB RAM
Disk	512 GB Disk	1200 GB Disk	1200 Disk	3600 GB Disk
Virtual NICs	2 vmxnet3 interfaces	2 vmxnet3 interfaces	2 vmxnet3 interfaces	2 vmxnet3 interfaces

Virtual appliance requirements

Endpoint Security virtual appliances require the following VMware resources:

- VMware ESXi host version 6.0 or later. Earlier ESXi versions are not supported
- VMware vSphere Client
- VMXNET 3 network drivers
- Standard virtual switch created for the monitoring ports of the virtual appliances, and attached to a physical network adapter on the ESXi server.
- VMware VCenter Server (recommended). When using vSphere Client to add virtual appliances to vCenter Server, the Deploy OVG Template wizard provides an easy way to enter activation code. Otherwise, you must type it in the virtual appliance console, because you cannot paste into this console.

ВЯРНО С ОРИГИНАЛА

Table 2. Physical appliance specifications.

Model Name	HX4502 or HX4502-D
Maximum Endpoints Managed	100,000
Form Factor	1U
CPU Description	E3-1240 v5, 4c, 3.5GHz
CPU Count	1
Memory Description	DDR4 ECC UDIMM 16GB, 2133MHz
DIMM Quantity	4
Total Memory (GB)	64
Motherboard Interface Ports	2x 1GigE BaseT, 1x IPMI, 2x USB2 (rear), 2x USB3 (rear), 1x DB9 Serial, 1x VGA
Addon Modules	TPM 1.2 (9655 4.34)
Addon Cards	LSI9341-4i, 2x 1GigE BaseT
Effective Storage Capacity	8TB
Storage Quantity	4
Unit Storage Capacity	4TB
Storage Type	HDD, 3.5", SAS3, 7.2krpm
RAID Types	RAID 10
Chassis Dimensions WxDxH inch (mm)	17.2in (437mm) x 25.6in (650mm) x 1.7in (43.2mm)
Chassis Weight lbs (Kg)	30.0 lbs. (13.6Kg)
As-shipped Packaged WxDxH in (mm)	34.5in (880mm) x 23.5in (600mm) x 9.25in (180mm)
As-shipped Packaged Weight lbs. (Kg)	41.0lbs. (18.6Kg)
Thermal Max Power BTU / Hr. (W)	836BTU / Hr (245W)
PSU	Redundant (1+1) 750 watt, 100 - 240 VAC 8.0 - 4.5A, 50-60 Hz IEC60320-C14 inlet, FRU
MTBF (Hrs.)	54,200
Compliance Safety	UL 60950-1-2014; CAN/; CSA C22.2 No. 60950-1-07; Am.1:2011+Am.2:2014; AS/NSZ 60950.1- 2011
Compliance EMC	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN55022 Class A; VCCI V-3 Class A; EN 55024; EN61000-3-2 Class A; EN 61000-3-3; CNS 13438 (2006) Class A; CISPR22 Class A; AS/NZS CISPR 22 Class A; KN 32; KN 35
Environmental Compliance	RoHS; REACH; WEEE
Operating Temperature	32 - 95° F (0 - 35° C)
Operating Humidity	10 - 95% @ 40° C, non-condensing
Non-Operating Temperature	-40 - 158° F (-40 - 70° C)
Non-Operating Humidity	10 - 95% @ 60° C, non-condensing
Operating Altitude	5000 ft. (1524 m.)

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. EP-EXT-DS-US-EN-000023-02

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™

ВЯРНО С ОРИГИНАЛА

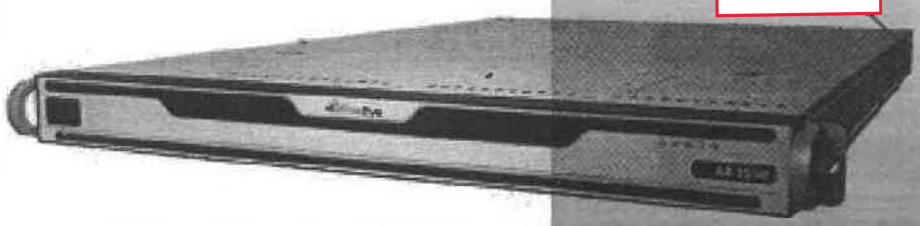
Продуктова брошура

Malware Analysis

Анализирайте атаките с 360-градусова видимост

ЦЕНТИ

- Извършва задълбочен криминалистичен анализ през пълния жизнен цикъл на атаката, използвайки софтуера FireEye MVX
- Оптимизира и събира анализ на подозрителен уеб код, изпълними и други файлове
- Предоставя подробен анализ на промени на системно ниво при операционни системи приложения върху файлови системи, памет и регистри
- Предлага анализ в реално време или sandbox анализ за потвърждаване на непознати нападения
- Динамично генерира информация за заплахи за незабавна локална защита чрез интеграция с FireEye Central Management
- Събира мрежови пакети, за да позволи анализ на злонамерена URL сесия и изпълнение на код
- Включва FireEye AV-Suite за оптимизиране на приоритизирането на отговор на инциденти
- Включва поддръжка за Windows и MacOS X среди



Фигура 1. FireEye Malware Analysis AX 5550 устройство.

Общо представяне

FireEye Malware Analysis е решение за криминалистичен анализ, което дава на анализаторите на сигурността контрол върху мощни автоматично конфигурирани тестови среди за безопасно изпълнение и инспектиране на атаки за напреднал вирусен софтуер, непознати и напреднали постоянни заплахи (APT), вградени в уеб страници, документи прикачени в имейли и файлове.

Тъй като киберпрестъпниците приспособяват атаките, за да проникнат в конкретен бизнес, потребителски акаунт или система, анализаторите се нуждаят от лесни за използване криминалистични инструменти, които им помагат бързо да се справят с целенасочените злонамерени дейности.

Оценка на атаките върху операционни системи, браузър и приложения

Malware Analysis използва FireEye Multi-Vector Virtual Execution™ (MVX) софтуер, за да предостави на анализаторите на компанията пълен 360-градусов поглед върху на атака, от първоначалното ѝ проникване до опитите за обратни сигнали към хакерски командни центрове и проследяване на бинарни опити за изтегляне.
Чрез предварително конфигурирана среда за виртуални анализи на Microsoft Windows и Apple MacOS X, MVX софтуерът изпълнява изцяло подозрителен код, за да позволи дълбока проверка на общи уеб обекти, документи прикачени в имейли и файлове.
Malware Analysis използва MVX механизма за проверка на единични файлове или файлови масиви за вирусен софтуер и проследява опити за изходяща връзка в множество протоколи.

Повече време за анализиране, а не за администриране

Malware Analysis освобождава администраторите от времеемката настройка, определяне на оптимално работно състояние и възстановяване на средите на виртуалните машини, използвани при ръчния анализ на вирусен софтуер. С вградена персонализация и подробен контрол върху изпълнението на зловреден код в тестовата среда, Malware Analysis позволява на криминалистичните анализатори да постигнат по-бързо и по-лесно разбиране за атаката, което да отговаря на нуждите на организацията.

0002447

ЕТ „Л и С - Стилияна Махалджийска"
Офис „Изток": 1113 София, ул. Жолио Кюри 46Б, тел./факс: 02 963 44 04
Офис „Младост 1": 1784 София, бул. Йерусалим, бл. 54, офис 11, партер (в двора), тел./факс: 02 974 57 55
Офис „Бизнес парк София": 1715 София, Бизнес парк София, сграда 8, вх. А - Б, тел.: 02 489 81 55
ET „L&S - Stiliyana Mahaldjiiska"
Office „Istok": 1113 Sofia Bulgaria, 46B, Fr. J. Curie Str., tel./fax: 02 963 44 04
Office „Mladost 1": 1784 Sofia Bulgaria, 54, Yerusalim Blvd., Office 11, ground floor, tel./fax: 02 974 57 55
Office „Business Park Sofia": 1715 Sofia Bulgaria, Business Park Sofia, building 8, ent. A-B, tel.: +359 2 489 81 55
office@variante.info
sliai@abv.bg
+359 888 875 932
www.variante.info

...ерете между анализ в реално време и sandbox ...нализ

Malware Analysis предоставя на потребителите два режима на анализ – анализ в реално време и sandbox анализ. Анализаторите на вирусен софтуер използват режима в реално време в мрежата за пълен анализ на жизнения цикъл на вирусния софтуер, позволявайки външно свързване. Това дава възможност на Malware Analysis да проследява напреднали атаки през няколко етапа и различни вектори. В режим sandbox пътят на изпълнение на конкретни образци на вирусен софтуер е напълно спрян и видим във виртуалната среда.

И в двата режима потребителите могат да генерират динамичен и анонимен профил на атаката, който може да бъде споделен чрез FireEye Central Management на други FireEye решения. Профилите за атака на вирусен софтуер, генерирани от Malware Analysis, включват идентификатори на код за вирусен софтуер, експлоатират URL адреси и други източници на заразяване и атаки. Също така характеристиките на протокола за комуникация на вирусен софтуер се споделят, за да осигурят динамично блокиране на опитите за извличане на данни в цялата мрежа на FireEye на организацията чрез FireEye Dynamic Threat Intelligence ™ (DTI).

YARA-базирани правила позволяват персонализиране

Malware Analysis поддържа импортиране на персонализирани YARA правила, за да се определят правилата на ниво байт и бързо да се анализират подозрителни обекти за заплахи, специфични за организацията.

Глобална мрежа за защита от вирусен софтуер

Malware Analysis може автоматично да споделя криминалистични данни за вирусен софтуер с други решения на FireEye чрез Централно управление, да блокира опитите за извличане на изходящи данни и да спре входящите познати атаки. Данните за заплаха от Malware Analysis могат да се споделят чрез облака на FireEye DTI, за да се постигне защита от нови възникващи атаки.

Чрез предварително конфигурираните FireEye MVX софтуери, елиминиращи необходимостта от финна настройка на следствения анализ, Malware Analysis спестява време на администраторите за настройка и решаване на проблеми с конфигурацията. Това решение също така помага на анализаторите на заплахите да анализират напреднали целенасочени атаки, без да добавят още мрежи и управление на сигурността.

Таблица 1. Технически спецификации.

	AX 5550
Производителност *	До 8,200 анализа на ден
Поддържани операционни системи	Microsoft Windows / Apple Mac OSX
Портове за мрежов интерфейс	2x 10/100/1000BASE-T порта
IPMI Порт (заден панел)	Включен
Клавиатура	Включена
DB15 VGA Портове (заден панел)	Включени
USB Порт (заден панел)	4x Type A USB порта
Сериен порт (заден панел)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Капацитет на диска	2x 4 TB HDD, RAID 1, 3.5 inch, FRU
Кутия	1RU, Fits 19 inch Rack
Размери на шасито (ШхДхВ)	17.2in(437mm) x 25.6in(650mm) x 1.7in(43.2mm)
DC захранване	Не е налично
AC захранване	Redundant (1+1) 750 watt, 100–240 VAC, 8–4.5A, 50–60 Hz, IEC60320-C14 inlet, FRU
Максимална консумация на енергия	225 вата
Максимално излъчване на топлина	768 BTU/h

Mahaldjiiska * Sofia L&S София ЕТ "ЛиС - Ст. Махалджийска"

…блица 1. Технически спецификации.

	AX 5550
MTBF	54,200 h
Тегло само на устройството / на доставения пакет lb. (kg)	26.8 lbs (12.2 kg) / 37.8 (17.2 kg)
Сертификати за сигурност	IEC 60950, EN 60950, CSA 60950-00, CE Marking
EMC/EMI сертификати	FCC (Part 15 Class-A), CE (Class-A), CNS, AS/NZS, VCCI(Class A)
Съответствие на нормативната уредба	RoHS, REACH, WEEE
Работна температура	0–40° C (32–104° F)
Работна относителна влажност	10–95% @ 40° C, без кондензация
Работна височина	3000 m / 9842 ft

Забележка: Показателите за производителността се базират на времената за анализ по подразбиране при използване на анализ на вирусен софтуер, но ще варират в зависимост от конфигурацията на системата и профилите на трафика, който се обработва.

За да научите повече за FireEye, посетете: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2019 FireEye, Inc Всички права запазени. FireEye е регистрирана търговска марка на FireEye, Inc. Всички други марки, продукти или услуги са или могат да бъдат търговски марки или марки на услуги на съответните им собственици. NS-EXT-DS-US-EN-000077-02

За FireEye, Inc.
FireEye е компания за интелигентна охрана. Работейки като безпроблемно, мащабируемо разширение на защитните операции на клиентите, FireEye предлага единна платформа, която съчетава иновативни технологии за сигурност, информация заплахи на национално ниво и световно призната консултация Mandiant®. С този подход FireEye елиминира сложността и тежестта на киберсигурността за организации, които се борят да се подготвят, предотвратяват и реагират на кибератаки.

FIREEYE

Sofia L&S София
ЕТ "ЛиС - Ст. Махалджийска"

Подписаната, [redacted] ЕГН: [redacted] Потвърждение №: 18ПР-1398/26.02.2018 г., удостоверявам верността на превода от английски на български език на приложения документ –, извършен от мен. Преводът се състои от 4 страници.

Подпис: [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

FIREEYE™

DATA SHEET

Malware Analysis

Analyze attacks with 360-degree visibility

HIGHLIGHTS

- Performs deep forensic analysis through the full attack life cycle, using the FireEye MVX engine
- Streamlines and batches analysis of suspicious web code, executables and files
- Reports in-depth on system-level OS and application changes to file systems, memory and registries
- Offers live-mode or sandbox analysis to confirm zero-day exploits
- Dynamically generates threat intelligence for immediate local protection via integration with FireEye Central Management
- Captures packets to allow analysis of malicious URL session and code execution
- Includes the FireEye AV-Suite to streamline incident response prioritization
- Includes support for Windows and MacOS X environments

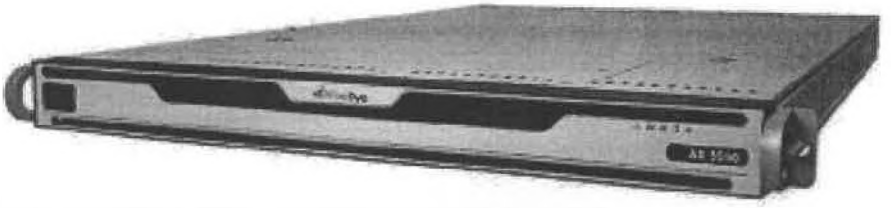


Figure 1. FireEye Malware Analysis AX 5550 appliance.

Overview

FireEye Malware Analysis is a forensic analysis solution that gives security analysts hands-on control over powerful auto-configured test environments to safely execute and inspect advanced malware, zero-day and advanced persistent threat (APT) attacks embedded in web pages, email attachments and files.

As cyber criminals tailor attacks to penetrate a specific business, user account or system, analysts need easy-to-use forensic tools that help them rapidly address targeted malicious activities.

Assess OS, browser and application attacks

Malware Analysis uses the FireEye Multi-Vector Virtual Execution™ (MVX) engine to provide in-house analysts with a full 360-degree view of an attack, from the initial exploit to callback destinations and follow on binary download attempts.

Through a pre-configured, instrumented Microsoft Windows and Apple MacOS X virtual analysis environment, the MVX engine fully executes suspicious code to allow deep inspection of common web objects, email attachments and files. Malware Analysis uses the MVX engine to inspect single files or batches of files for malware and tracks outbound connection attempts across multiple protocols.

Spend time analyzing, not administering

Malware Analysis frees administrators from time-consuming setup, baselining and restoration of the virtual machine environments used in manual malware analysis. With built-in customization and granular control over payload detonations, Malware Analysis uses enables forensic analysts to arrive at a comprehensive understanding of the attack that is suited to the needs of the enterprise.

ВЯРНО С ОРИГИНАЛА

Choose live analysis or sandbox modes
Malware Analysis provides users with two analysis modes— live and sandbox. Malware analysts use the live, on-network mode for full malware life cycle analysis, allowing external connectivity. This gives Malware Analysis the ability to track advanced attacks across multiple stages and different vectors. In sandbox mode, the execution path of particular malware samples is fully contained and visible in the virtual environment.

In both modes, users can generate a dynamic and anonymized profile of the attack that can be shared through FireEye Central Management to other FireEye solutions. The malware attack profiles generated by Malware Analysis includes identifiers of malware code, exploit URLs and other sources of infections and attacks. Also, malware communication protocol characteristics are shared to provide dynamic blocking of data exfiltration attempts across the organization's entire FireEye deployment via FireEye Dynamic Threat Intelligence™ (DTI).

YARA-based rules enables customization
Malware Analysis supports custom YARA rules importation to specify byte-level rules and quickly analyze suspicious objects for threats specific to the organization.

Global malware protection network
Malware Analysis can automatically share malware forensics data with other FireEye solutions via Central Management, block outbound data exfiltration attempts and stop inbound known attacks. Threat data from Malware Analysis can be shared via the FireEye DTI cloud to protect against new emerging attacks.

With pre-configured FireEye MVX engines eliminating the need for tuning heuristics, Malware Analysis saves administrators setup time and configuration issues. This solution also helps threat researchers analyze advanced targeted attacks without adding network and security management overhead.

Table 1. Technical specifications.

	AX 5550
Performance *	Up to 8,200 Analyses Per Day
OS Support	Microsoft Windows / Apple Mac OSX
Network Interface Ports	2x 10/100/1000BASE-T Ports
IPMI Port (rear panel)	Included
Keypad	Included
DB15 VGA ports (rear panel)	Included
USB Ports (rear panel)	4x Type A USB Ports
Serial Port (rear panel)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Drive Capacity	2x 4 TB HDD, RAID 1, 3.5 inch, FRU
Enclosure	1RU, Fits 19 inch Rack
Chassis Dimensions (WxDxH)	17.2in(437mm) x 25.6in(650mm) x 1.7in(43.2mm)
DC Power Supply	Not Available
AC Power Supply	Redundant (1+1) 750 watt, 100-240 VAC, 8-4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU
Power Consumption Maximum	225 watts
Thermal Dissipation Maximum	768 BTU/h

ВЯРНО С ОРИГИНАЛА

Table 1. Technical specifications.

	AX 5550
MTBF	54,200 h
Appliance Alone / As Shipped Weight lb. (kg)	26.8 lbs (12.2 kg) / 37.8 (17.2 kg)
Safety Certifications	IEC 60950, EN 60950, CSA 60950-00, CE Marking
EMC/EMI Certifications	FCC (Part 15 Class-A), CE (Class-A), CNS, AS/NZS, VCCI(Class A)
Regulatory Compliance	RoHS, REACH, WEEE
Operating Temperature	0–40° C (32–104° F)
Operating Relative Humidity	10–95% @ 40° C, non-condensing
Operating Altitude	3000 m / 9842 ft

Note: Performance numbers are based on default analysis times when using the Malware Analysis, but will vary depending on the system configuration and traffic profiles being processed.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. NS-EXT-DS-US-EN-000077-02

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™

ВЯРНО С ОРИГИНАЛА

Stiliyana Mahaldjiiska
L&S EYE™
TRANSLATION OFFICE

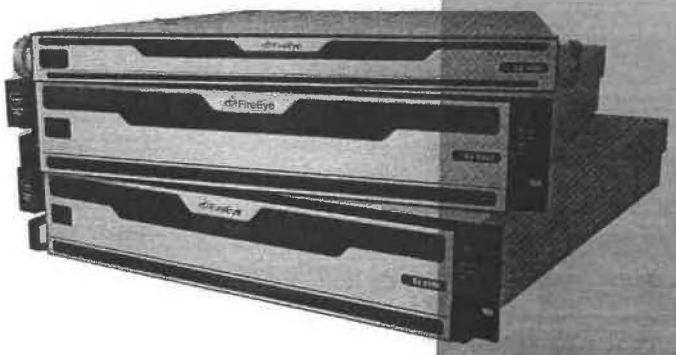
Продуктова брошура

FireEye Email Security Server Edition

Адаптивна, интелигентна, мащабируема защита срещу заплахи, изпращани по имейл

АКЦЕНТИ

- Предлага цялостна защита на електронната поща срещу прикачени файлове с вирус, URL адреси с фишинг, спуфинг, непознати и многоетапни атаки
- Поддържа анализ на операционни системи Microsoft Windows и Apple macOS X
- Детайлно изследва имейла за заплахи, скрити в защитени с парола файлове, криптирани прикачени файлове и URL адреси
- Придобива разузнавателна информация за заплахите в реално време от FireEye DTI Cloud
- Приоритизира и спира заплахи, като предоставя контекстна информация за сигналите
- Внедрява се локално с интегрирана или разпределена MVX услуга



Фигура 1. Интегрираните устройства за защита на електронната поща включват EX 3500, EX 5500 и EX 8500.

Общо представяне

Имейлът е най-уязвимият вектор за кибер атаки, тъй като има най-големия обем на входящи данни. Организациите са изправени пред все по-голям брой предизвикателства за сигурността от напреднали заплахи, базирани на имейл. Повечето напреднали заплахи използват електронна поща, за да доставят URL адреси, свързани със сайтове за фишинг и прикачени файлове с вируси. Тъй като е широко използвана и има възможности за персонализиране, електронната поща е основната среда за кибер престъпления.

FireEye Email Security помага на организациите да намалят до минимум риска от скъпоструващи нарушения, причинени от напреднали имейл атаки. Внедрен локално, FireEye Email Security - Server Edition е сред първите в индустрията в идентифицирането, изолирането и незабавното спиране на атаките, базирани на URL и прикачени файлове, преди да влязат в средата на организацията. Email Security съчетава контекст, ръководен от информация, и допълнения за засичане, за да открие злонамерени и безопасни фишинг URL адреси, базирайки се на платформа за обработка на големи данни. Multi-Vector Virtual Execution™ (MVX) софтуерът без дефиниции анализира прикачени файлове и URL адреси, свързани със съдържание за сваляне, срещу изчерпателна кръстосана матрица на операционни системи, приложения и уеб браузъри. Заплахите се идентифицират с минимално смущение като почти няма фалшиви положителни резултати.

0002449

ЕТ „Л и С - Стилияна Махалджийска"
Офис „Изток": 1113 София, ул. Жолио Кюри 46Б, тел./факс: 02 963 44 04
Офис „Младост 1": 1784 София, бул. Йерусалимски бл. 54, офис 11, партер (74 57 55
Офис „Бизнес парк София": 1715 София, Бизнес парк София, сграда 8, вх.
ET „L&S - Stiliyana Mahaldjiiska"
Office „Istok": 1113 Sofia Bulgaria, 46B, Fr. J. Curie Str., tel./fax: 02 963 44 04
Office „Mladost 1": 1784 Sofia Bulgaria, 54, Yerusalim Blvd., Office 11, ground floor, tel./fax: 02 974 57 55
Office „Business Park Sofia": 1715 Sofia Bulgaria, Business Park Sofia, building 8, ent. A-B, tel.: +359 2 489 81 55

office@variante.info
sliai@abv.bg
+359 888 875 932
www.variante.info

ра обширна информация за заплахите чрез ния за нарушения от първа ръка и милиони сензори. urity използва както конкретни доказателства, така и стуална информация за атаки и нападатели, за да даде ритет на сигналите и да блокира заплахите в реално време.

ез интегриране с FireEye Network Security и Endpoint Security ганизациите могат да получат по-широка видимост на ноговекторни смесени атаки и да координират защитата в ално време.

щита срещу заплахи, получавани от имейл
цялата лична информация, налична онлайн, берпрестъпникът може да използва социален инженеринг, за подмами почти всеки потребител да предприеме действие, да тисне върху URL адрес или да отвори прикачен файл.

nail Security осигурява откриване и предотвратяване в реално еме на опити за извличане на данни за вписване, атаки, ползващи представяне с чужда самоличност, както и фишинг аки, които обикновено заобикалят традиционните защити на ектронната поща. Имейлите се анализират и карантинират локират), ако се открият неизвестни и напреднали заплахи:

ид прикачени файлове, включително, но не само: EXE, DLL, DF, SWF, DOC / DOCX, XLS / XLSX, PPT / PPTX, JPG, PNG, MP3, MP4 ZIP / RAR / TNEF архиви

щитени с парола и криптирани прикачени файлове

щитени с парола прикачени файлове с парола изпратена чрез зображение

RL адреси, вградени в имейли, документи на MS Office, PDF и рхивни файлове (ZIP, ALZIP, JAR) и други типове файлове Juencoded, HTML)

айлове, изтеглени чрез URL адреси - и дори FTP линкове

амаскирани, подправени, съкратени и динамично пренасочени RL адреси

нализ на URL адреси с фишинг и от тип typosquatting

еизвестни изображения на операционни системи Microsoft Vindows и Apple macOS X, уязвимости на браузъра и приложенията

ирусен код, вграден в имейли, част от spear-phishing атака

Дои атаките на ransomware започват с имейл, обикновено се изисква обратно връщане към сървър за командване и контрол за криптиране на данните. Защитата по имейл идентифицира и спира тези трудно разпознаваеми многоетапни кампании за вирусен софтуер.

Откриване на заплахи от ново поколение
Email Security помага за намаляване на риска от скъпоструващи нарушения чрез идентифициране и изолиране на напреднали, целенасочени и други скрити атаки, прикрити като нормален трафик. След като бъдат открити, тези атаки се спират незабавно, анализират се и получават идентификация за по-бързо разпознаване на бъдещи заплахи.

В основата на Email Securityса Разширената URL защита, MVX софтуерът и MalwareGuard. Тези технологии използват машинно обучение и анализ за идентифициране на атаки, които заобикалят традиционните защити, основани на дефиниции и политики.
Като неразделна част от Advanced URL Defense, PhishVision е софтуер за класификация на изображения, който използва задълбочено обучение за компилиране и сравняване на скрийншоти на надеждни и често таргетирани марки спрямо уеб страници, на които се позовават URL адреси в имейл. Работейки заедно с PhishVision, Kraken е плъгин за откриване на фишинг, който прилага анализ на съдържанието на домейни и страници за увеличаване на машинното обучение. Skyfeed, още един напредък в откриването на URL адреси, е целенасочена, напълно автоматизирана система за събиране на вирусен софтуер. Акаунти, блогове, форуми и публикации в социални медии се събират, за да се открият зловредни съобщения, които грешно се улавят като доброкачествени (False Negative). Многоаспектната природа на Advanced URL Defense предлага на организациите, защитени чрез Email Security, безпрецедентна защита срещу извличане на данни за вписване и spear-phishing атаки.

MalwareGuard е помощна машина за машинно обучение, която приема бинарни файлове като входяща информация и извежда оценка на подозрителността. Всеки преносим изпълним файл (PE), засечен в мрежата, се анализира от MalwareGuard. Взема се решение въз основа на резултата и откритията, задействани от MalwareGuard, получават име.

MVX софтуерът открива непознати, многопоточни и други скрити атаки, като използва динамичен анализ без дефиниции в безопасна, виртуална среда. Той идентифицира непознати атаки и вирусен софтуер, за да спре заразяването и компрометирането.

Предотвратяване на атаки използващи evasion техники за избягване на алгоритмите за засичане
Email Security поддържа функция за контролиран режим на работа, за да се защитава от атаки, които избягват заявки за отдалечени обекти. MVX софтуерът открива вирусен софтуер, изискващ много изтегляния и връща отдалечените обекти, поискани от примерния двоичен файл. Контролираният режим на работа намалява фалшивите негативи за многоетапни изтегляния, напреднали spear-phishing атаки и напреднали ransomware атаки.
Нападателите също се опитват да избегнат технологията, използвана за откриване на подозрителни URL адреси. Като част от Advanced URL Defense, справянето с техники за избягване от засичане на фишинг сайтове непрекъснато се развива. Функциите за засичане на evasion техники са подсилени от Advanced URL Defense технологията. Като друга методлогия за откриване на evasion техники за избягване от засичане, виртуалните машини на решението могат да бъдат персонализирани така, че да имитират „използвана" крайна точка, когато се изпълнява потенциално злонамерен обект. Много техники на избягване се предотвратяват, като се гарантира, че виртуалните машини имитират реален домейн на крайна точка, потребител на домейн, данни на Outlook и история на браузъра.

ия за подобряване на ефективността на обработката алите

Security анализира всеки имейл с прикачен файл и адрес, за да идентифицира точно днешните модерни аки. Актуализациите в реално време от цялата екосистема за защита на FireEye, комбинирани с приписване на сигнали на известни участници, изпращащи заплахи, предоставят контекст за приоритизиране и отговор на критични сигнали както и блокиране на напреднали имейл атаки. Известните, неизвестните и не базираните на вирусен софтуер заплахи се идентифицират с минимално смущение и фалшиви положителни резултати, така че ресурсите да бъдат фокусирани върху реални атаки с цел намаляване на оперативните разходи. Категоризирането на рисковия софтуер отделя истинските опити за нарушение от нежеланата, но не толкова злонамерена дейност (като рекламен и шпионски софтуер), за да се даде приоритет на отговора на сигнала.

Бърза адаптация към развиващата се среда на заплахите

Email Security помага на Вашата организация по-бързо да адаптира Вашата проактивна защита срещу заплахи, пренасяни по електронна поща, чрез разузнавателна информация за заплахите в реално време от облака FireEye Dynamic Threat Intelligence (DTI). Дълбокото разузнаване на заплахите и нападателите съчетава информация за атакуващите и потърпевшите, както и за засегнатите машини:

- Осигурява навременна и по-широка видимост на заплахите
- Идентифицира специфични възможности и функции на открит вирусен софтуер и прикачени файлове с вирус
- Предоставя контекстуална информация за приоритизиране и ускоряване на реакцията
- Определя вероятната идентичност и мотиви на нападателя и проследява неговите действия в рамките на Вашата организация
- Пренаписва всички URL адреси, вградени в имейл, за да защити потребителите от злонамерени връзки
- Ретроактивно идентифицира spear-phishing атаки и предотвратява достъпа до фишинг сайтове, като подчертава злонамерени URL адреси

Интегриране на работния процес за отговор

Email Security работи безпроблемно с FireEye Helix и FireEye Central Management.

- Като компонент на платформата за операции за сигурност — FireEye Helix — осигурява видимост в цялата инфраструктура. FireEye Helix увеличава сигнали от имейли и трети страни чрез информация, корелация на крайна точка, автоматизация и съвети за разследване. С тези възможности FireEye Helix идентифицира непознати заплахи и дава възможност за експертни решения.
- Централното управление корелира сигналите както от защитата на електронната поща, така и от мрежовата сигурност с цел по-широк поглед върху атака и задаване на правила за блокиране, за да се предотврати разпространението на атаката.
- Централното управление поддържа етикетиране въз основа на роли, за да знае кой е бил целта.
- Централното управление поддържа реакция на сигнали и отстраняване въз основа на критерии, базирани на ролите.

Допълнителни възможности

Базирани на YARA правила позволяват персонализиране

Email Security позволява на анализаторите да определят и тестват персонализирани правила за анализ на прикачени файлове в имейли за заплахи, насочени към тяхната организация.

Защита срещу атаки, представящи се с чужда самоличност

Email Security – Server Edition предлага възможност за блокиране на компрометирането на бизнес имейл (BEC), за да защити важните служители от измама. Създава се политика, която сравнява показваните имена на входящите имейли с одобрен списък, който съвпада с одобрените податели.

Опашка за съобщения, управление на сигналите и карантина

Email Security – Server Edition осигурява висока степен на контрол върху имейл съобщенията, които сканира. За активно разгръщане на режима на защита, съобщенията могат да бъдат проследявани и управлявани, докато се движат по MTA опашката. Атрибутите на електронната поща могат да се използват за търсене и проверка дали съобщенията са получени, анализирани и доставени до следващата точка от мрежата, а тенденциите във времето могат да бъдат наблюдавани чрез интуитивно табло. Изчерпателните списъци за разрешаване и блокиране осигуряват персонализиран контрол върху обработката на имейли. Могат да се търсят и избират общи атрибути за сигнализиране. Могат да се извършват действия едновременно с множество вдигнати аларми и със съобщения, поставени под карантина.

Режим на активна защита или само за наблюдение

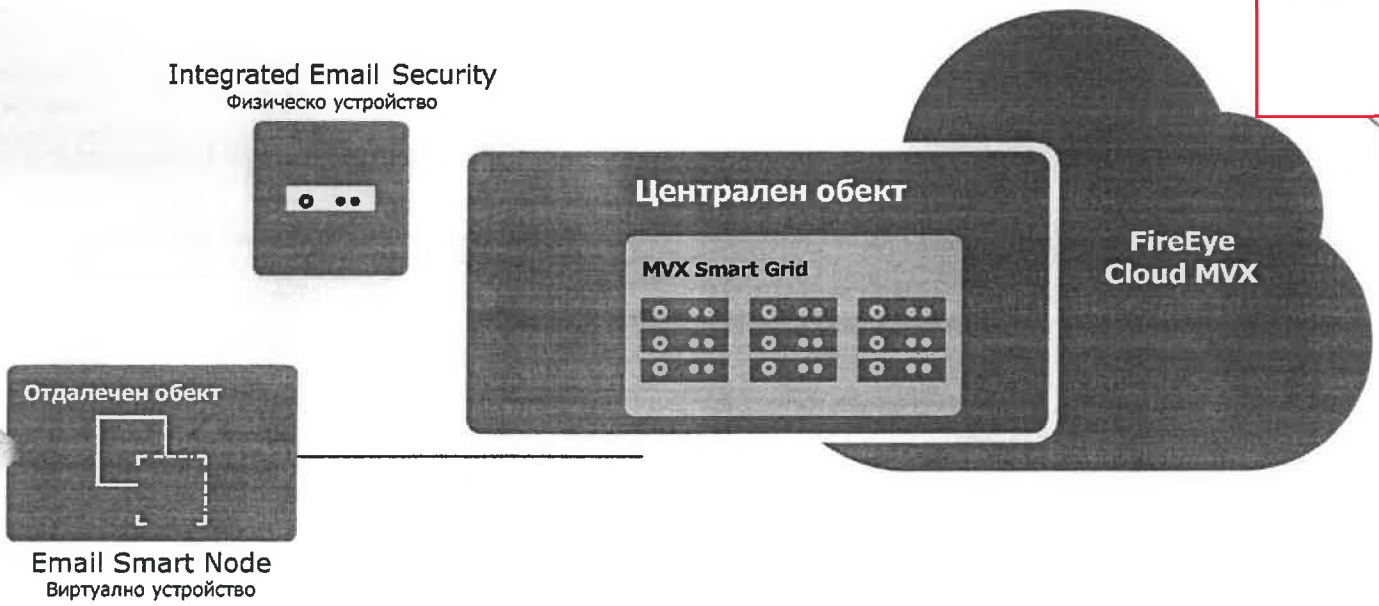
Email Security може да анализира имейли и да поставя под карантина съобщения със заплахи, за да предостави активна защита. Когато искат само наблюдение, организациите могат да използват решението в прозрачен BCC режим, за да се изпращат копия от имейли до Email Security за анализ.

ви опции за внедряване

il Security – Server Edition предлага различни ции за внедряване, за да отговори на нуждите и бюджета на организацията:

- **Integrated Email Security:** самостоятелно, многофункционално хардуерно устройство с интегрирана MVX услуга за осигуряване на точка за влизане на електронна поща в един сайт. FireEye Email Security е лесно за управление решение, което се внедрява за по-малко от 60 минути. Не изисква правила, политики или настройка.
- **Distributed Email Security:** разширяеми уреди с централно споделена MVX услуга за осигуряване на точки за влизане на електронна поща в организациите
- **Email Smart Node:** виртуалните сензори анализират трафика на електронната поща, за да открият и блокират злонамерен трафик и да подадат подозрителна активност по криптирана връзка към услугата MVX за окончателен анализ на случая
- **MVX Smart Grid:** локална, централно разположена, еластична MVX услуга, която предлага прозрачна мащабируемост, вградено N + 1 отклонение и автоматизирано балансиране на натоварването.

  Пускането от интегриран хардуерен уред в MVX Smart Grid осигурява допълнителен капацитет за откриване и анализ на заплахи, пренасяни по имейл по време на пикови периоди на получаване на съобщения.
- **FireEye Cloud MVX:** Абонамент за услуга MVX, който гарантира поверителност чрез анализ на трафика на Email Smart Node. Само съмнителни обекти се изпращат по криптирана връзка към услугата MVX, при която обекти, разкрити като доброкачествени, се отхвърлят.



Фигура 2. Разпространени и включени модели на внедряване на Email Security.

[redacted]

ица 1. Технически спецификации.

	EX 3500	EX 5500	EX 8500
Производителност*	До 700 уникални прикачени файлове на час	До 1,800 уникални прикачени файлове на час	До 2,650 уникални прикачени файлове на час
Портове на мрежов интерфейс	2x 1GigE BaseT	2x 1GigE BaseT	4x SFP+ (supporting 10GigE Fiber, 10GigE Copper, 1GigE Copper), 2x 1GigE BaseT
Портове за управление	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
IPMI наблюдение	Включено	Включено	Включено
VGA Порт (заден панел)	Включен	Включен	Включен
USB Портове (заден панел)	4x USB Type A заден	2x USB Type A преден 2x USB Type A заден	2x USB Type A преден 2x USB Type A заден
Сериен порт (заден панел)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
апацитет на паметта	4x 2TB, RAID 10, HDD 3.5 inch, FRU	4x 2TB, RAID 10, HDD 3.5 inch, FRU	4x 2TB, RAID 10, HDD 3.5 inch, FRU
Кутия	1RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack
Размери на шасито (ШхДхВ)	17.2" x 25.6" x 1.7" (437 x 650 x 43.2 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)
AC Захранване	Redundant (1+1) 750 watt, 100 - 240 VAC, 9 – 4.5A,50-60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC, 9 – 4.5A,50-60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC, 9 – 4.5A,50-60 Hz, IEC60320-C14 inlet, FRU
DC Захранване	Не е налично	Не е налично	Не е налично
Максимална топлинна мощност	245 вата (836 BTU на час)	456 вата (1,556 BTU на час)	530 вата (1,808 BTU на час)
MTBF (h)	54,200 часа	57,401 часа	53,742 часа
Тегло само на устройството / на доставения пакет, lb (kg)	30.0 lbs (13.6 kg) / 41.0 lbs (18.6 kg)	44.1 lbs (20.0 kg) / 65.3 lbs (29.6 kg)	44.4 lbs (20.2 Kg) / 65.6 lbs (29.8 kg)
Отговаряне на изискванията за сигурност	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
тговаряне на EMC изискванията	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015
Сертификати за сигурност	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1
Съответствие с изискванията за опазване на околната среда	RoHS Directive 2011/65/EU; REACH; WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU; REACH; WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU; REACH; WEEE Directive 2012/19/EU
Работна температура	0 ~ 35° C (32 ~ 95° F)	0 ~ 35° C (32 ~ 95° F)	0 ~ 35° C (32 ~ 95° F)
Работна относителна влажност	10 ~ 95% @ 40° C, без кондензация	10 ~ 95% @ 40° C, без кондензация	10 ~ 95% @ 40° C, без кондензация
Работна височина	3,000 m / 9,842 ft	3,000 m / 9,842 ft	3,000 m / 9,842 ft

* Всички стойности на производителността варират в зависимост от системната конфигурация и профила за трафик на електронната поща, която се обработва. Размерът на устройството (ата) е въз основа на уникални прикачени документи на час.

[redacted] [redacted] [redacted] [redacted] [redacted]

ца 2. FireEye MVX smart grid спецификации.

	VX 5500	VX 12500
Поддържани операционни системи	Microsoft Windows Apple macOS X	Microsoft Windows Apple macOS X
Производителност *	До 480 уникални прикачени файлове на час	До 3,780 уникални прикачени файлове на час
Висока достъност **	N+1	N+1
Портове за управление (заден панел)	1x 10/100/1000 Mbps BASE- T Ports	1x 10/100/1000 Mbps BASE- T Ports
Клъстерни портове (заден панел)	3x 10/100/1000 Mbps BASE-T Ports	1x 10/100/1000 Mbps BASE-T Ports, 2x 10 Gbps BASE-T Ports
IPMI Порт (заден панел)	Включен	Включен
Преден LCD и клавиатура	Не са налични	Включени
VGA Портове	Включени	Включени
USB портове (заден панел)	4x Type A USB Ports	2x Type A USB Ports
Сериен порт (заден панел)	115,200 bps, No Parity, 8 bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Капацитет на диска	2x 2TB 3.5 SAS HDD, RAID 1, hot-swappable, FRU	4 x 4TB 3.5" SAS3 HDD, RAID 1, FRU
Кутия	1RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack
Размери на шасито (ШхДхВ)	17. 2x25.6x1.7 Inches (437 x 650 x 43.2 mm)	17.2x33.5x3.5 Inches (437 x 851 x 89 mm)
DC Захранване	Не е налично	Не е налично
AC Захранване	Redundant (1+1) 750 watt, 100-240VAC, 8 - 3.8 A, 50-60 Hz, IEC60320-C14, inlet, hot-swappable, FRU	Redundant (1+1) 800W: 100-127V, 9.8A-7A 1000W: 220-240V, 7-5A, 50-60Hz, FRU IEC60320-C14 inlet, FRU
Максимална консумация на енергия	285 вата	760 вата
Максимално излъчване на топлина	972 BTU на час	2594 BTU на час
MTBF	54,200 часа	38,836 часа
Тегло само на устройството / на доставения пакет	33 lb (15 kg) / 48 lb (21.8 kg)	46 lb (21 kg) / 90 lb (40.2 kg)
Сертификати за сигурност	FIPS 140-2 Level 1, CC NDPP v1.1	FIPS 140-2 Level 1, CC NDPP v1.1
Безопасност в съответствие на нормативната уредба	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

* Всички стойности на производителността варират в зависимост от системната конфигурация и профила на трафика, който се обработва.

** Чрез използване на подходящи допълнителни хардуерни устройства.

ЕТ "Л&С - Ст. Махалджийска" * ЕТ "ЛиС - St. Mahaldjiiska" * Sofia L&S София

Таблица 3. FireEye Email Security smart node, спецификации на виртуалния сензор.

	EX 5500V
Поддържани операционни системи	Microsoft Windows, Apple macOS X
Производителност *	Up to 1,250 unique attachments per hour
Мрежови портове за мониторинг	2
Мрежови портове за управление	2
CPU ядра	8
Памет	16 GB
Капацитет на диска	384 GB
Мрежови адаптери	VMXNet 3, vNIC
Поддръжка на хипервизор	VMWare ESXi 6.0 или по-нова версия

* Всички стойности на производителността варират в зависимост от системната конфигурация и профила на трафика, който се обработва.

За да научите повече за FireEye, посетете: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2019 FireEye, Inc. Всички права запазени. FireEye е регистрирана търговска марка на FireEye, Inc. Всички други марки, продукти или услуги са или могат да бъдат търговски марки или марки на услуги на съответните им собственици. E-EXT-DS-US-EN-000044-02

За FireEye, Inc.
FireEye е компания за интелигентна охрана. Работейки като безпроблемно, мащабируемо разширение на защитните операции на клиентите, FireEye предлага единна платформа, която съчетава иновативни технологии за сигурност, информация заплахи на национално ниво и световно призната консултация Mandiant®. С този подход FireEye елиминира сложността и тежестта на киберсигурността за организации, които се борят да се подготвят, предотвратяват и реагират на кибератаки.

FIREEYE

Подписаната, [redacted], ЕГН: [redacted], Потвърждение №: 18ПР-1398/26.02.2018 г., удостоверявам верността на превода от английски на български език на приложения документ –, извършен от мен. Преводът се състои от 8 страници.

Подпис: [redacted]

ЕТ "ЛиС - Ст. Махалджийска" • ЕТ "L&S - St. Mahaldjiiska" • Sofia • L&S • София

FIREEYE™

DATA SHEET

FireEye Email Security Server Edition

Adaptive, intelligent, scalable defense against email borne threats

HIGHLIGHTS

- Offers comprehensive email security against malicious attachments, credential-phishing URLs, spoofing, zero-day and multi-stage attacks
- Supports analysis against Microsoft Windows and Apple macOS X operating system images
- Extensively examines email for threats hidden in password-protected files, encrypted attachments, and URLs
- Acquires real-time threat intelligence from the FireEye DTI Cloud
- Prioritizes and contains threats by providing contextual insights for alerts
- Deploys on-premises with integrated or distributed MVX service

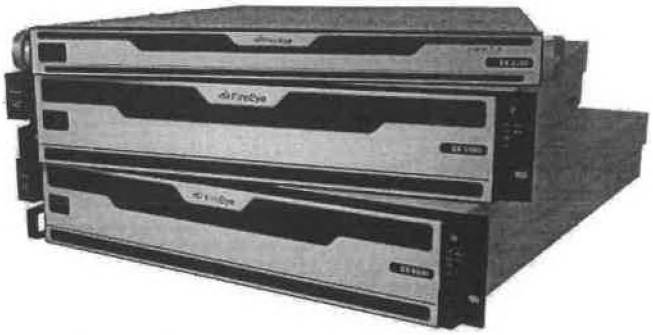


Figure 1. Integrated Email Security appliances include EX 3500, EX 5500 and EX 8500.

Overview

Email is the most vulnerable vector for cyber attacks because it is the highest volume data ingress point. Organizations face an ever-increasing number of security challenges from email-based advanced threats. Most advanced threats use email to deliver URLs linked to credential phishing sites and weaponized file attachments. Because it is highly targetable and customizable, email is the primary medium for cyber crime.

FireEye Email Security helps organizations minimize the risk of costly breaches caused by advanced email attacks. Deployed on premises, FireEye Email Security – Server Edition leads the industry in identifying, isolating and immediately stopping URL and attachment-based attacks, before they enter an organization's environment. Email Security combines intelligence-led context and detection plug-ins to unearth malicious and benign phishing URLs on a big data, scalable platform. The signatureless Multi-Vector Virtual Execution™ (MVX) engine analyzes email attachments and URLs linked to downloadable content against a comprehensive cross-matrix of operating systems, applications and web browsers. Threats are identified with minimal noise, and false positives are nearly nonexistent.

ВЯРНО С ОРИГИНАЛА

FireEye collects extensive threat intelligence on adversaries through firsthand breach investigations and millions of sensors. Email Security draws on both concrete evidence and contextual intelligence about attacks and attackers to prioritize alerts and block threats in real time.

By integrating with FireEye Network Security and Endpoint Security organizations can get broader visibility into multi-vector blended attacks and coordinate real-time protection.

Defense against email borne threats
With all the personal information available online, a cyber criminal can use social engineering to trick almost any user into taking an action, clicking a URL or opening an attachment.

Email Security provides real-time detection and prevention against credential harvesting, impersonation and spear-phishing attacks that typically evade traditional email security defenses. Emails are analyzed and quarantined (blocked) if unknown and advanced threats are found hidden in:

- Attachment types including, but not limited to: EXE, DLL, PDF, SWF, DOC/ DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 and ZIP/RAR/TNEF archives
- Password-protected and encrypted attachments
- Password-protected attachments with password sent via image
- URLs embedded in emails, MS Office documents, PDF and archive files (ZIP, ALZIP, JAR), and other file types (Uuencoded, HTML)
- Files downloaded through URLs – and even FTP links
- Obfuscated, spoofed, shortened and dynamically redirected URLs
- Credential-phishing and typosquatting URLs
- Unknown Microsoft Windows and Apple macOS X operating system images, browser and application vulnerabilities
- Malicious code embedded in spear-phishing emails

While ransomware attacks start with an email, a call back to a command-and-control server is typically required to encrypt the data. Email Security identifies and stops these hard-to- detect multi-stage malware campaigns.

Superior threat detection
Email Security helps mitigate the risk of costly breaches by identifying and isolating advanced, targeted and other evasive attacks camouflaged as normal traffic. Once detected, these attacks are immediately stopped, analyzed and fingerprinted for faster identification of future threats.

At the core of Email Security are Advanced URL Defense, the MVX engine and MalwareGuard. These technologies use machine learning and analytics to identify attacks that evade traditional signature and policy-based defenses.

An integral part of Advanced URL Defense, PhishVision is an image classification engine that uses deep learning to compile and compare screenshots of trusted and commonly targeted brands against web pages referenced by URLs in an email. Working in tandem with PhishVision, Kraken is a phishing detection plug-in that applies domain and page content analytics to augment machine learning. Skyfeed, another advance in URL detection, is a purpose-built, fully automated malware intelligence gathering system. Social media accounts, blogs, forums and threat feeds are collected to discover false negatives. The multi-faceted nature of Advanced URL Defense offers organizations protected by Email Security unparalleled defense against credential harvesting and spear-phishing attacks.

MalwareGuard is a machine learning utility that takes binary files as input and outputs a suspiciousness score. Every Portable Executable (PE) file seen on the wire is analyzed by MalwareGuard. A decision is made based on the score and detections triggered by MalwareGuard are assigned a name.

The MVX engine detects zero-day, multi-flow and other evasive attacks by using dynamic, signature-less analysis in a safe, virtual environment. It identifies never-before-seen exploits and malware to stop infection and compromise.

Evasion mitigation
Email Security supports a controlled live mode feature to defend against attacks that evade requests for remote objects. The MVX engine detects malware requiring multiple downloads and returns the remote objects requested by the sample binary. Controlled live mode reduces false negatives for multistage downloads, advanced spear-phishing attacks and advanced ransomware intrusions.

Attackers also try to evade technology used for detecting suspicious URLs. As part of Advanced URL Defense, evasion mitigations for phishing sites are continually evolving. Evasion mitigations are continually enhanced as part of Advanced URL Defense. Another evasion mitigation, Guest Images can be customized to mimic a "used" endpoint when a potentially malicious object is executed. Many evasion techniques are prevented by ensuring the Guest Image reproduces an endpoint domain user, Outlook data and browser history.

ВЯРНО С ОРИГИНАЛА

Integration to improve alert handling efficiencies
Email Security analyzes every email attachment and URL to accurately identify today's advanced attacks. Real-time updates from the entire FireEye security ecosystem combined with attribution of alerts to known threat actors provide context for prioritizing and acting on critical alerts and blocking advanced email attacks. Known, unknown and non-malware-based threats are identified with minimal noise and false positives so that resources are focused on real attacks to reduce operational expenses. Riskware categorization separates genuine breach attempts from undesirable, but less malicious activity (such as adware and spyware) to prioritize alert response.

Rapid adaptation to the evolving threat landscape
Email Security helps your organization continually adapt your proactive defense against email-borne threats via real-time threat intelligence from the FireEye Dynamic Threat Intelligence (DTI) Cloud. Deep intelligence about threats and attackers combines adversarial, machine and victim intelligence to:

- Deliver timely and broader visibility to threats
- Identify specific capabilities and features of detected malware and malicious attachments
- Provide contextual insights to prioritize and accelerate response
- Determine the probable identity and motives of an attacker and track their activities within your organization
- Rewrite all URLs embedded within an email to protect users from malicious links
- Retroactively identify spear-phishing attacks and prevent access to phishing sites by highlighting malicious URLs

Response workflow integration
Email Security works seamlessly with FireEye Helix and FireEye Central Management.

- As a component of the security operations platform — FireEye Helix — it provides visibility across the entire infrastructure. FireEye Helix augments email and third-party alerts with intelligence, correlation to the endpoint, automation, and investigative tips. With these capabilities, FireEye Helix surfaces unseen threats and empowers expert decisions.
- Central Management correlates alerts from both Email Security and Network Security for a broader view of an attack and to set blocking rules to prevent the attack from spreading.
- Central Management supports role-based tagging to know who is being targeted.
- Central Management supports alert response and remediation based on role-based criteria.

Additional capabilities
YARA-based rules enable customization
Email Security enables analysts to specify and test custom rules to analyze email attachments for threats targeting their organization.

Executive impersonation protection
Email Security – Server Edition offers the capability to block business email compromises (BEC) to protect important employees from being spoofed. A policy is created that compares inbound email display names to an approved list that matches approved envelope senders.

Message queue, alert and quarantine management
Email Security – Server Edition provides a high degree of control over the email messages it scans. For active protection-mode deployments, messages can be tracked and managed as they move through the MTA queue. Email attributes can be used to search and verify that messages were received, analyzed and delivered to the next hop and trends over time can be monitored through an intuitive dashboard. Explicit allow and block lists provide custom control over email processing. Common alert attributes can be searched and selected. And bulk operations can be performed on alerts and quarantined messages.

Active-protection or monitor-only mode
Email Security can analyze emails and quarantine threats for active protection. For monitor-only deployments organizations just set up a transparent BCC rule to send copies of emails to Email Security for analysis.

ВЯРНО С ОРИГИНАЛА

Flexible Deployment Options

Email Security – Server Edition offers various deployment options to match an organization's needs and budget:

- **Integrated Email Security:** standalone, all-in-one hardware appliance with integrated MVX service to secure an email ingress point at a single site. FireEye Email Security is an easy-to-manage solution that deploys in under 60 minutes. It doesn't require rules, policies or tuning.
- **Distributed Email Security:** extensible appliances with centrally shared MVX service to secure email ingress points within organizations
- **Email Smart Node:** virtual sensors analyze email traffic to detect and block malicious traffic and submit suspicious activity over an encrypted connection to the MVX service for definitive verdict analysis
- **MVX Smart Grid:** on-premise, centrally located, elastic MVX service that offers transparent scalability, built-in N+1 fault tolerance and automated load balancing.

  Bursting from an integrated hardware appliance to an MVX Smart Grid provides added capacity for detecting and analyzing email-borne threats during peak message throughput periods.
- **FireEye Cloud MVX:** MVX service subscription that ensures privacy by analyzing traffic on the Email Smart Node. Only suspicious objects are sent over an encrypted connection to the MVX service, where objects revealed as benign are discarded.

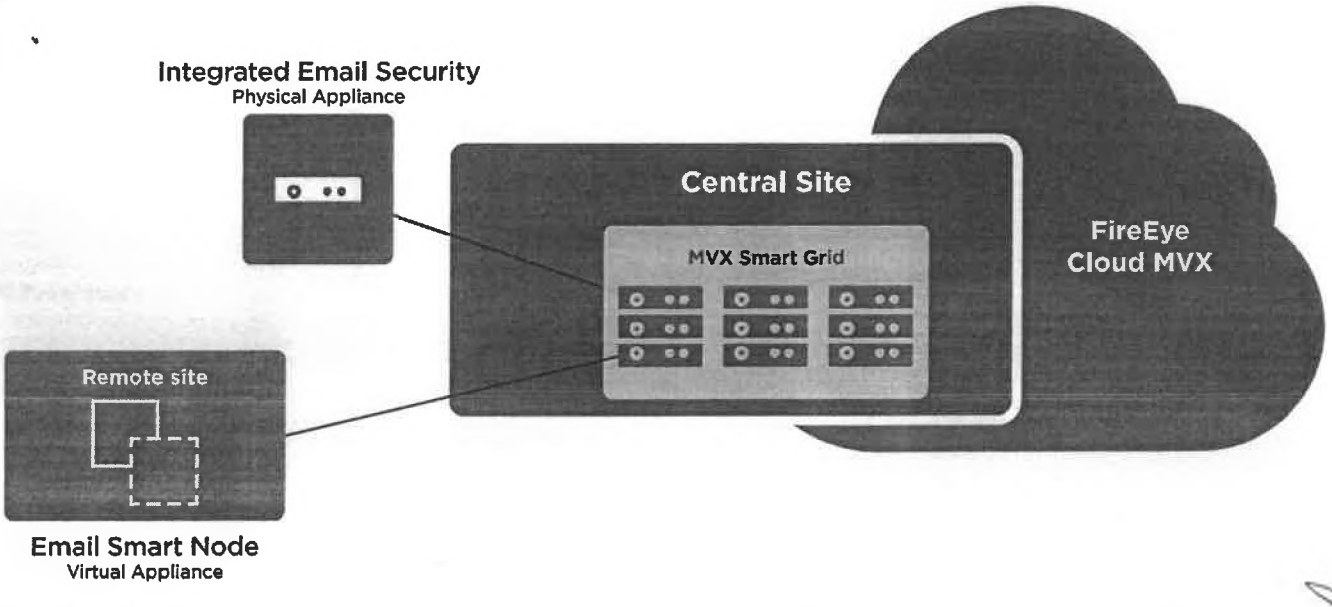


Figure 2. Distributed and bursting deployment models for Email Security.

ВЯРНО С ОРИГИНАЛА

Table 1. Technical specifications.

	EX 3500	EX 5500	EX 8500
Performance*	Up to 700 unique attachments per hour	Up to 1,800 unique attachments per hour	Up to 2,650 unique attachments per hour
Network Interface Ports	2x 1GigE BaseT	2x 1GigE BaseT	4x SFP+ (supporting 10GigE Fiber, 10GigE Copper, 1GigE Copper), 2x 1GigE BaseT
Management Ports	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
IPMI Monitoring	Included	Included	Included
VGA Port (rear panel)	Included	Included	Included
USB Ports (rear panel)	4x USB Type A Rear	2x USB Type A Front, 2x USB Type A Rear	2x USB Type A Front, 2x USB Type A Rear
Serial Port (rear panel)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Storage Capacity	4x 2TB, RAID 10, HDD 3.5 inch, FRU	4x 2TB, RAID 10, HDD 3.5 inch, FRU	4x 2TB, RAID 10, HDD 3.5 inch, FRU
Enclosure	1RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack
Chassis Dimensions (WxDxH)	17.2" x 25.6" x 1.7" (437 x 650 x 43.2 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)
AC Power Supply	Redundant (1+1) 750 watt, 100 - 240 VAC, 9 - 4.5A,50-60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC, 9 - 4.5A,50-60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC, 9 - 4.5A,50-60 Hz, IEC60320-C14 inlet, FRU
DC Power Supply	Not Available	Not Available	Not Available
Thermal Maximum Power	245 watts (836 BTU per hour)	456 watts (1,556 BTU per hour)	530 watts (1,808 BTU per hour)
MTBF (h)	54,200 hours	57,401 hours	53,742 hours
Appliance Alone / As Shipped Weight, lb (kg)	30.0 lbs (13.6 kg) / 41.0 lbs (18.6 kg)	44.1 lbs (20.0 kg) / 65.3 lbs (29.6 kg)	44.4 lbs (20.2 Kg) / 65.6 lbs (29.8 kg)
Compliance Safety	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Compliance EMC	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015
Security Certifications	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1
Environmental Compliance	RoHS Directive 2011/65/EU; REACH; WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU; REACH; WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU; REACH; WEEE Directive 2012/19/EU
Operating Temperature	0 - 35° C (32 - 95° F)	0 - 35° C (32 - 95° F)	0 - 35° C (32 - 95° F)
Operating Relative Humidity	10 - 95% @ 40° C, non-condensing	10 - 95% @ 40° C, non-condensing	10 - 95% @ 40° C, non-condensing
Operating Altitude	3,000 m / 9,842 ft	3,000 m / 9,842 ft	3,000 m / 9,842 ft

* All performance values vary depending on the system configuration and email traffic profile being processed. Size appliance(s) based on unique attachments per hour.

ВЯРНО С ОРИГИНАЛА

Table 2. FireEye MVX smart grid specifications.

	VX 5500	VX 12500
OS Support	Microsoft Windows Apple macOS X	Microsoft Windows Apple macOS X
Performance*	Up to 480 unique attachments per hour	Up to 3,780 unique attachments per hour
High Availability**	N+1	N+1
Management Ports (rear panel)	1x 10/100/1000 Mbps BASE- T Ports	1x 10/100/1000 Mbps BASE- T Ports
Cluster Ports (rear panel)	3x 10/100/1000 Mbps BASE-T Ports	1x 10/100/1000 Mbps BASE-T Ports, 2x 10 Gbps BASE-T Ports
IPMI Port (rear panel)	Included	Included
Front LCD & Keypad	Not Available	Included
VGA Ports	Included	Included
USB Ports (rear panel)	4x Type A USB Ports	2x Type A USB Ports
Serial Port (rear panel)	115,200 bps, No Parity, 8 bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Drive Capacity	2x 2TB 3.5 SAS HDD, RAID 1, hot-swappable, FRU	4 x 4TB 3.5" SAS3 HDD, RAID 1, FRU
Enclosure	1RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack
Chassis Dimensions (WxDxH)	17. 2x25.6x1.7 Inches (437 x 650 x 43.2 mm)	17.2x33.5x3.5 Inches (437 x 851 x 89 mm)
DC Power Supply	Not Available	Not Available
AC Power Supply	Redundant (1+1) 750 watt, 100-240 VAC, 8 - 3.8 A, 50-60 Hz, IEC60320-C14, inlet, hot-swappable, FRU	Redundant (1+1) 800W: 100-127V, 9.8A-7A 1000W: 220-240V, 7-5A, 50-60Hz, FRU IEC60320-C14 inlet, FRU
Power Consumption Maximum	285 watts	760 watts
Thermal Dissipation Maximum	972 BTU per hour	2594 BTU per hour
MTBF	54,200 hours	38,836 hours
Appliance Alone / As Shipped Weight	33 lb (15 kg) / 48 lb (21.8 kg)	46 lb (21 kg) / 90 lb (40.2 kg)
Security Certification	FIPS 140-2 Level 1, CC NDPP v1.1	FIPS 140-2 Level 1, CC NDPP v1.1
Regulatory Compliance Safety	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

* All performance values vary depending on the system configuration and traffic profile being processed.
** With appropriate redundant hardware configurations.

ВЯРНО С ОРИГИНАЛА

Table 3. FireEye Email Security smart node, virtual sensor specifications.

	EX 5500V
OS Support	Microsoft Windows, Apple macOS X
Performance*	Up to 1,250 unique attachments per hour
Network Monitoring Ports	2
Network Management Ports	2
CPU cores	8
Memory	16 GB
Drive Capacity	384 GB
Network Adapters	VMXNet 3, vNIC
Hypervisor Support	VMWare ESXi 6.0 or later

* All performance values vary depending on the system configuration and traffic profile being processed.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. E-EXT-DS-US-EN-000044-02

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™

ВЯРНО С ОРИГИНАЛА

Stiliyana Mahaldjiiska
FIREEYE™ TRANSLATION OFFICE

Превод от а

Продуктова брошура

File Protect

Откриване и премахване на вирусен софтуер в мрежови файлови споделени масиви и хранилища за съдържание

АКЦЕНТИ

- Намира скрит вирусен софтуер, който не може да бъде открит от традиционните AV приложения
- Активира карантина (режим на защита) или само анализ (режим на наблюдение)
- Осигурява рекурсивни, по график и по заявка сканирания на мрежови файлови споделени масиви, съвместими с CIFS и NFS
- Осигурява проактивна защита за Microsoft OneDrive и Sharepoint
- Включва анализ на широк спектър от файлове като PDF файлове, документи на Microsoft Office и мултимедийни файлове
- Интегрира се с FireEye Endpoint Security за рационализиране на приоритизирането на отговор на инциденти и определянето на конвенции
- Споделя данни за заплахата чрез FireEye Central Management и облака FireEye DTI

Общо представяне

FireEye File Protect защитава набора от данни в широк спектър от типове файлове срещу атаки, които произхождат от уеб поща, онлайн инструменти за прехвърляне на файлове, облака и преносими устройства за съхранение на файлове. Такива атаки могат да се разпространят чрез мрежови файлови споделени масиви и хранилища за съдържание. File Protect анализира мрежовите файлови споделени масиви и хранилищата за управление на съдържание, за да открие и карантира вирусен софтуер, който заобикаля защитните стени от ново поколение, IPS, AV и gateways.

Предизвикателства от вирусния софтуер при споделяне на файлове

Днешните съвременни кибер атаки използват усъвършенстван вирусен софтуер и тактика за напреднали постоянни з[illegible] (APT), за да проникнат в защитите и да се разпространяват странично чрез мрежови файлови споделени масиви и хранилища за съдържание. Това дава възможност на вирусния софтуер да се установи дългосрочно в мрежата и да зарази множество системи, дори и офлайн. Много корпоративни центрове за данни остават особено уязвими за напреднал вирусен софтуер, базиран на съдържание, тъй като традиционните защити са неефективни срещу тези атаки, които често влизат в мрежата чрез позволените канали за комуникация. Киберпрестъпниците използват тези уязвимости за разпространение на вирусен софтуер в мрежови файлови споделени масиви и за вграждане на вирусен код в огромни хранилища за данни, което води до постоянна заплаха дори след отстраняване.

Значение на защитата на съдържанието на файловете

Без начин за откриване на неактивен вирусен софтуер в съдържанието напредналите постоянни заплахи могат да използват мрежови активи, за да извличат лична информация и да причинят значителни щети. File Protect анализира файлови дялове и хранилища на корпоративно съдържание, използвайки патентования FireEye Multi-Vector Virtual Execution™ (MVX) софтуер, който открива непознат злонамерен код, вграден в общи типове файлове (PDF, MS Office, vCards, ZIP / RAR / TNEF и т.н.) и мултимедийно съдържание (QuickTime, MP3, Real Player, JPG, PNG и т.н.). File Protect извършва рекурсивни, по график и по заявка сканирания на мрежови файлови споделени масиви и хранилища за съдържание, за да се идентифицира и карантира вирусен софтуер. Това спира ключов етап от жизнения цикъл на напредналите атаки.

ЕТ „Л и С[illegible]ияна Махалджийска“
Офис „Изток“: 11[illegible] Жолио Кюри 46Б, тел./факс: 02 963 44 04
Офис „Младост 1“[illegible] бул. Йерусалим, бл. 54, офис 11, партер ([illegible]74 57 55
Офис „Бизнес парк София“: 1715 София, Бизнес парк София, сграда 8, вх.[illegible]
ЕТ „L&S - Stiliyana Mahaldjiiska“
Office „Istok“: 1113 Sofia Bulgaria, 46B, Fr. J. Curie Str., tel./fax: 02 963 44 04[illegible]
Office „Mladost 1“: 1784 Sofia Bulgaria, 54, Yerusalim Blvd., Office 11, ground[illegible]55
Office „Business Park Sofia“: 1715 Sofia Bulgaria, Business Park Sofia, buildin[illegible] 489 81 55

0002446

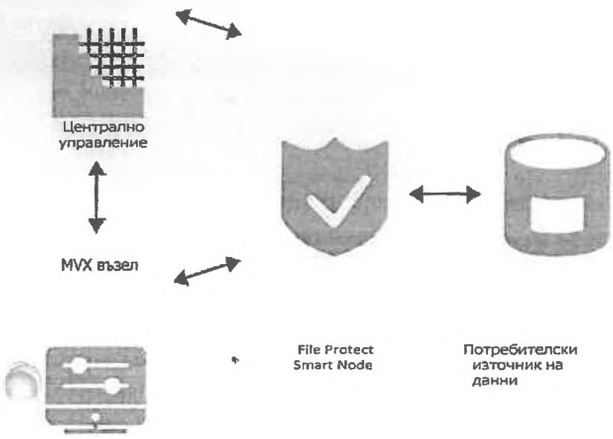
office@variante.info
sliai@abv.bg
+359 888 875 932
www.variante.info

...иване на неизвестни заплахи

...Eye FX използва FireEye MVX софтуер, за да ...спектира всеки файл и да потвърди наличието на непозната експлоатация или вирусен код. FireEye MVX софтуерът открива непознати атаки, многопоточни и други скрити атаки с динамичен анализ без използване на дефиниции във виртуална среда.
Той спира фазите на инфекция и компрометиране от етапите за изпълнение на кибер атаките, като идентифицира непознати експлоатации и вирусен софтуер.

Силата на MVX Smart Grid

Smart Grid FireEye MVX подобрява мрежовата сигурност на FireEye с гъвкава и мащабируема архитектура на внедряване чрез хибриден или частен облак. MVX Smart Grid използва иновативен подход за по-ефективно осигуряване на кампуси, клонове и отдалечени потребители, като отделя MVX софтуера от хардуера и виртуалните Smart Nodes. ™ Smart Nodes анализират интернет тафик, за да открият и блокират заплахите с помощта на различни техники като статичен анализ, анализи, IPS, приложна информация и други, докато MVX софтуерът извършва основен динамичен анализ.



Защита за Microsoft OneDrive и SharePoint

File Protect непрекъснато сканира съдържание, за да предупреди и карантинира трайно вирусен софтуер, открит в хранилищата на OneDrive и SharePoint. Платформата използва протокол WebDAV за сигурна интеграция с услуги на SharePoint за защита на работните процеси в предприятието, които използват SharePoint хранилища.

Правилата, базирани на YARA, позволяват персонализиране

File Protect поддържа персонализирани YARA правила за анализ на големи количества заплахи за файлове, специфични за организацията.

Опростено приоритизиране на инцидентите

С FireEye Endpoint Security всеки злонамерен обект може да бъде допълнително анализиран, за да се определи дали антивирусните доставчици са успели да открият вирусния софтуер, спрян от File Protect. Това дава възможност на организациите да приоритизират ефикасно последващите действия при реакции на инциденти и да използват общи конвенции за определяне на известни вирусни програми.

Споделяне на вирусен софтуер

Получената динамично генерирана информац... заплаха в реално време може да помогне на всички продукти на FireEye да защитят локалната мрежа чрез интеграция с централното управление.
Тази информация може да бъде споделена в глобален мащаб чрез облака FireEye Dynamic Threat Intelligence (DTI), за да уведомява всички абонати за възникващи заплахи.

Без настройка на правила и почти нулеви фалшиви положителни резултати

За разлика от IPS системите, File Protect не изисква абсолютно никаква настройка. Гъвкавите режими на внедряване включват мониторинг само с анализ и активна карантина. Това дава възможност на компаниите да научат колко вирусен софтуер има в мрежови файлови споделени масиви и активно да спрат страничното разпространение на вирусен софтуер.

Content Smart Notes за защита, когато е необходимо

С FireEye Content Smart Nodes, мениджърите на съдържанието и сигурността получават гъвкаво, виртуално решение за защита на критично съдържание в цялата фирма. В съчетание с MVX Smart Grid, защитата на съдържанието се надгражда и се разгръща безпроблемно до мястото, където е необходима.

Гъркави фактори

Идеален за всяка мрежова среда, клиентите могат да избират между виртуални FireEye Content Smart Nodes или традиционни локално разположени хардуерни устройства.

ЕТ "L&S - St. Mahaldjiiska" Sofia L&S София ЕТ "ЛиС - Ст. Махалджийска"

...а 1. FireEye Content Smart Node.

	FX 2500V
...ддържана операционна система	Microsoft Windows, MacOS X
Производителност	40,000 файла/ден
Портове за мрежов интерфейс	Ether 1, Ether 2
CPU ядра	2
Памет	8 GB
Капацитет на диска	512 GB
Поддържане на Hypervisor	VMWare ESXi 6.0 или по-нова

Таблица 2. FireEye технически спецификации.

	FX 6500
Производителност *	До 70,000 файла на ден
Портове на мрежов интерфейс	4x 1GigE BaseT
IPMI порт (заден панел)	Включен
USB портове (заден панел)	2x USB Type A отпред, 2x USB Type A отзад
Сериен порт (заден панел)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Капацитет на съхранение	4x 2TB, RAID 10, HDD 3.5 inch, FRU
...гия	2RU, Fits 19 inch Rack
Размери на шасито (ШхДхВ)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)
Захранване	Redundant (1+1) 800 watt, 100 - 240 VAC, 9 – 4.5A,50-60 Hz, IEC60320-C14 inlet, FRU
Максимална консумация на енергия	530 watts
Максимално топлинно разсейване	1,808 BTU/h
MTBF	53,742 h
Само уреда / В опаковка lb. (kg)	44.4 lbs (20.2 Kg) / 65.6 lbs (29.8 kg)
Сертификати за безопасност	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
EMC/EMI Сертификати	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015
...азване на нормативната уредба	RoHS Directive 2011/65/EU; REACH; WEEE Directive 2012/19/EU
Работна температура	0–40° C (32–104° F)
Работна относителна влажност	10–95% @ 40° C, без кондензация
Работна височина	3,000 m / 9,842 ft

За да научите повече за FireEye, посетете: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2019 FireEye, Inc. Всички права запазени. FireEye е регистрирана търговска марка на FireEye, Inc. Всички други марки, продукти или услуги са или могат да бъдат търговски марки или марки на услуги на съответните им собственици. NS-EXT-DS-US-EN-000054-03

За FireEye, Inc.

FireEye е компания за интелигентна охрана. Работейки като безпроблемно, мащабируемо разширение на защитните операции на клиентите, FireEye предлага единна платформа, която съчетава иновативни технологии за сигурност, информация заплахи на национално ниво и световнопризната консултация Mandiant®. С този подход FireEye елиминира сложността и тежестта на киберсигурността за организации, които се борят да се подготвят, предотвратяват и реагират на кибератаки.

FIREEYE™

ЕТ "L&S - St. Mahaidjiiska" Sofia L&S София ЕТ "ЛиС - Ст. Махаджийска"

Подписаната, [redacted], ЕГН: [redacted], Потвърждение №: 18ПР-1398/26.02.2018 г., удостоверявам верността на превода от английски на български език на приложения документ –, извършен от мен. Преводът се състои от 4 страници.

Подпис: [redacted]

ЕТ "L&S - St. Manaldjiiska" * ЕТ "ЛиС - Ст. Мехаджийска" * Sofia L&S София

[redacted]

[redacted]

[redacted]

[redacted]

FIREEYE™

DATA SHEET

File Protect

Detect and eliminate malware on file shares and content stores

HIGHLIGHTS

- Finds latent malware undetected by traditional AV engines
- Deploys in active quarantine (protection mode) or analysis only (monitor mode)
- Provides recursive, scheduled and on-demand scans of CIFS and NFS compatible file shares
- Provides proactive protection for Microsoft OneDrive and Sharepoint
- Includes analysis of a wide range of file types such as PDFs, Microsoft Office documents and multimedia files
- Integrates with FireEye Endpoint Security to streamline incident response prioritization and naming conventions
- Shares threat data through FireEye Central Management, and the FireEye DTI cloud

Overview

FireEye File Protect secures data assets across a wide range of file types against attacks that originate from web mail, online file transfer tools, the cloud and portable file storage devices. Such attacks can spread to file shares and content repositories. File Protect analyzes network file shares and content management stores to detect and quarantine malware that bypass next generation firewalls, IPS, AV and gateways.

Challenges of malware on file shares

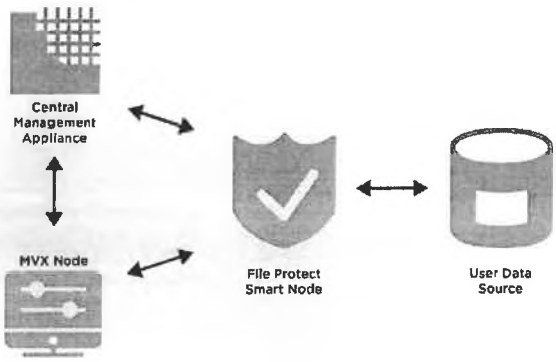
Today's advanced cyber attacks use sophisticated malware and advanced persistent threat (APT) tactics to penetrate defenses and spread laterally through file shares and content repositories. This enables malware to establish a longterm foothold in the network and infect multiple systems, even those offline. Many corporate data centers remain especially vulnerable to advanced, content-based malware because traditional defenses are ineffective against these attacks, which often enter the network through legitimate means. Cyber criminals leverage these vulnerabilities to spread malware into network file shares and embed malicious code in vast data stores, resulting in a persistent threat even after remediation.

Importance of file content protection

Without a way to detect resting malware in content, APTs can exploit network assets to extract proprietary information and cause significant damage. File Protect analyzes file shares and enterprise content repositories using the patented FireEye Multi-Vector Virtual Execution™ (MVX) engine that detects zero-day malicious code embedded in common file types (PDF, MS Office, vCards, ZIP/RAR/TNEF, etc.) and multimedia content (QuickTime, MP3, Real Player, JPG, PNG, etc.). File Protect performs recursive, scheduled and on-demand scanning of accessible network file shares and content stores to identify and quarantine resident malware. This halts a key stage of the advanced attack life cycle.

Revealing unknown, zero-day threats
FireEye FX uses the FireEye MVX engine to inspect each file and confirm the existence of zero-day exploits or malicious code. The FireEye MVX engine detects zero-day, multi-flow and other evasive attacks with dynamic, signature-less analysis in a safe, virtual environment. It stops infection and compromise phases of the cyber attack kill chain by identifying neverbefore seen exploits and malware.

The Power of MVX Smart Grid
FireEye MVX Smart Grid improves on FireEye Network Security with a flexible and scalable deployment architecture via hybrid or private cloud. MVX Smart Grid uses an innovative approach to more effectively secure campuses, branch offices and remote users by separating the MVX engine from hardware and virtual Smart Nodes.™ Smart Nodes analyze Internet traffic to detect and block threats using a variety of techniques such as static analysis, analytics, IPS, applied intelligence, and more, while the MVX engine performs core dynamic analysis.



Protection for Microsoft OneDrive and SharePoint
File Protect continuously scans content to alert and permanently quarantine malware discovered in OneDrive and SharePoint repositories. The platform leverages WebDAV protocol to securely integrate with SharePoint services to protect enterprise business workflows that use SharePoint repositories.

YARA-based rules enable customization
File Protect supports custom YARA rules to analyze large quantities of file threats specific to the organization.

Streamlined incident prioritization
With FireEye Endpoint Security, each malicious object can be further analyzed to determine if antivirus vendors were able to detect the malware stopped by File Protect. This enables organizations to efficiently prioritize incident response follow-ups and use common naming conventions for known malware.

Malware intelligence sharing
The resulting dynamically generated, real-time threat intelligence can help all FireEye products protect the local network through integration with Central Management. This intelligence can be shared globally through the FireEye Dynamic Threat Intelligence (DTI) cloud to notify all subscribers of emerging threats.

No rules tuning and near-zero false positives
Unlike IPS systems, File Protect requires absolutely no tuning. Flexible deployment modes include analysis-only monitoring and active quarantining. This enables companies to learn how much malware is resident on file shares and to actively stop the lateral spread of malware.

Content Smart Notes for protection where needed
With FireEye Content Smart Nodes, content and security managers gain a flexible, virtual solution to protect missioncritical content throughout the enterprise. Coupled with the MVX Smart Grid, content protection scales and deploys seamlessly to where it is needed.

Flexible form factors
Ideal for any network environment, customers can choose between either virtual FireEye Content Smart Nodes or traditional on-premise hardware appliances.

Table 1. FireEye Content Smart Node.

	FX 2500V
OS Support	Microsoft Windows, MacOS X
Performance	40,000 files/day
Network Interface Ports	Ether 1, Ether 2
CPU Cores	2
Memory	8 GB
Drive Capacity	512 GB
Hypervisor Support	VMWare ESXi 6.0 or later

ВЯРНО С ОРИГИНАЛА

Table 2. FireEye technical specifications.

	FX 6500
Performance *	Up to 70,000 Files per day
Network Interface Ports	4x 1GigE BaseT
IPMI Port (rear panel)	Included
USB Ports (rear panel)	2x USB Type A Front, 2x USB Type A Rear
Serial Port (rear panel)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Storage Capacity	4x 2TB, RAID 10, HDD 3.5 inch, FRU
Enclosure	2RU, Fits 19 inch Rack
Chassis Dimensions (WxDxH)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)
AC Power Supply	Redundant (1+1) 800 watt, 100 - 240 VAC, 9 - 4.5A,50-60 Hz, IEC60320-C14 inlet, FRU
Power Consumption Maximum	530 watts
Thermal Dissipation Maximum	1,808 BTU/h
MTBF	53,742 h
Appliance Alone / As Shipped Weight lb. (kg)	44.4 lbs (20.2 Kg) / 65.6 lbs (29.8 kg)
Safety Certifications	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
EMC/EMI Certifications	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015
Regulatory Compliance	RoHS Directive 2011/65/EU; REACH; WEEE Directive 2012/19/EU
Operating Temperature	0-40° C (32-104° F)
Operating Relative Humidity	10-95% @ 40° C, non-condensing
Operating Altitude	3,000 m / 9,842 ft

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. NS-EXT-DS-US-EN-000054-03

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™

ВЯРНО С ОРИГИНАЛА

Stiliyana Mahaldjiiska

ENDPOINT SECURITY

TRANSLATION OFFICE

ОТКРИВАНЕ И ЗАЩИТА СРЕЩУ НЕИЗВЕСТЕН ЗАПЛАХИ В КРАЙНИ ТОЧКИ И РАБОТА С ВГРАДЕНА ИНФОРМАЦИЯ ЗА ЗАПЛАХИ

С FireEye Endpoint Security (серия HX) организациите могат активно да проверяват, анализират и спират известни и неизвестни заплахи във всяка крайна точка.

АКЦЕНТИ

- Разширяване на интегрираната FireEye Threat Intelligence от ядрото до крайната точка за цялостна защита срещу напреднали заплахи
- Провеждане на подробни проучвания на крайни точки, за да се идентифицират и спрат IOC и да се създадат срокове за реагиране на събития с Triage Viewer
- Откриване, идентифициране и спиране на заплахи за десетки хиляди крайни точки (свързани или не) за минути чрез Enterprise Security Search
- Лесно оценяване на дейностите на крайните точки за идентифициране на атаки и предупреждение на анализаторите
- Отговаря на общите критерии и държавните стандарти
- Централизиране на хост-базирани работни процеси на едно място за текущи сигнали, подробности за системата и придобивания
- Бързо реагиране на известни и неизвестни заплахи с критична контекстуална информация
- Защита на всички крайни точки, независимо дали са в помещението или извън него, извън мрежата или зад превода на мрежови адреси (NAT)
- Спиране на заплахи и компрометирани устройства с едно натискане, като същевременно позволява дистанционно разследване

- Днешните квалифицирани нападатели заобикалят традиционната защита, на която повечето екипи по сигурността разчитат от години, за да защитят крайните си точки. Дори когато традиционната защита спре известна заплаха, тя не може да определи какво е опитала да направи тази заплаха. FireEye Endpoint Security помага на Вашия екип по сигурността да проследи и спре известни и неизвестни напреднали заплахи срещу крайните точки, като използва функции като:
- Triage Viewer, за преглед на познати индикатори за компрометиране (IOCs)
- Enterprise Security Search за бързо сканиране и спиране на заплахи
- Data Acquisition за задълбочена проверка и анализ на крайните точки
- Exploit Guard, който разчита на години на разузнаване на заплахи за откриване на експлоатационни процеси в крайните точки

ET „L&S - St. Mahaldjiiska" * „Ст. Махалджийска" * ET „L&S - Sofia София" * 0002

FireEye

ET „Л и [redacted] яна Махалджийска"
Офис „Изток": [redacted] олио Кюри 46Б, тел./факс: 02 963 44 04
Офис „Младост 1": 1784 София, бул. Йерусалим, бл. 54, офис 11, партер (в двора), тел./факс: 02 974 57 55
Офис „Бизнес парк София": 1715 София, Бизнес парк София, сграда 8, вх. А - Б, тел.: 02 489 81 55

ET „L&S - Stiliyana Mahaldjiiska"
Office „Istok": 1113 Sofia Bulgaria, 46B, Fr. J. Curie Str., tel./fax: 02 963 44 04
Office „Mladost 1": 1784 Sofia Bulgaria, 54, Yerusalim Blvd., Office 11, ground floor, tel./fax: 02 974 57 55
Office „Business Park Sofia": 1715 Sofia Bulgaria, Business Park Sofia, building 8, ent. A-B, tel.: +359 2 489 81 55

office@variante.info
sliai@abv.bg
+359 888 875 932
www.variante.info

...РЕТЕ ИНФОРМАЦИЯТА ...ПЛАХИ КЪМ ВСЯКА ...АЙНА ТОЧКА

За да бъде ефективна, на мястото на атаката трябва да има информация за заплахата. Endpoint Security безпроблемно разширява възможностите за разузнаване на заплахите на други продукти на FireEye до крайната точка. Ако продукт на FireEye открие атака някъде в мрежата, крайните точки се актуализират автоматично и се проверяват за IOC.

ПОСТИГНЕТЕ ПОДОБРЕНА ВИДИМОСТ НА КРАЙНИТЕ ТОЧКИ

...имостта е от решаващо значение за идентифициране на първопричината за сигнал и Ви позволява да извършвате задълбочени анализи на заплахата. Кешът за проверка в Endpoint Security Ви позволява да инспектирате и анализирате настоящи и минали мрежови сигнали (включително тези от SIEM) в крайната точка. Triage Viewer Ви предоставя автоматично събрана времева линия от събития за всяка крайна точка.

ОТКРИЙТЕ СКРИТИ ЗЛОВРЕДНИ ПРОЦЕСИ В КРАЙНИТЕ ТОЧКИ

...таките, използващи скрити уязвимости на крайните точки, затрудняват традиционните решения за защита на крайни точки (EPP), които се фокусират върху една дейност от една крайна точка. Exploit Guard е гъвкава информационна функция за експлоатация, която осигурява откриване и реакция на крайни точки (EDR) и предпазва от атаките, които традиционните решения за крайни точки пропускат. Използвайки информация за експлоатацията натрупана с десетилетия от софтуера на FireEye MVX, функцията Exploit Guard позволява на серията HX да оценява множество на пръв поглед различни дейности в една или повече крайни точки, за да се определи дали има експлоатация.

ПОЛУЧАВАТЕ ПЪЛНО ПОКРИТИЕ НА КРАЙНАТА ТОЧКА

Крайните точки на място и тези отдалечени извън организационната мрежа са ключови уязвими точки. Endpoint Security обхваща всички крайни точки, като подава информация на IOC към тях, независимо от типа на интернет връзката. Това Ви позволява да проучвате и спирате крайни точки навсякъде по света, без да се нуждаете от допълнителни VPN връзки.

СПИРАНЕ НА КОМПРОМИРАНИ КРАЙНИ ТОЧКИ И ПРЕДОТВРАТЯВАНЕ НА СТРАНИЧНО РАЗПРОСТРАНЕНИЕ

Атаките, които започват в една крайна точка, могат бързо да се разпространят през Вашата мрежа. След като идентифицирате атака, Endpoint Security Ви позволява незабавно да изолирате компрометирани устройства, за да спрете атаката и да предотвратите страничното разпространение - всичко с едно натискане на бутона. След това можете да проведете пълно криминалистично разследване на инцидента, без да рискувате по-нататъшно заразяване.

КАК РАБОТИ ENDPOINT SECURITY

FireEye Endpoint Security използва разузнавателна информация за заплахите, за да съпостави сигналите, генерирани от мрежовите платформи за сигурност на FireEye, събраните логове от системите, както и продуктите за мрежова сигурност с IOC на всяка крайна точка. След като бъде потвърдена заплахата, Endpoint Security може да проучи десетки хиляди крайни точки за минути и да изолира компрометирани крайни точки с едно натискане на бутона, докато оценявате допълнителни потенциални рискове.

С Endpoint Security можете да разберете:

- Кои вектори е използвала атаката за проникване във Вашата система
- Дали атаката се разпространила странично към други системи
- Дали има атака на конкретна крайна точка и дали тя продължава
- Колко дълго е била компрометирана крайна точка (и)
- Дали даден IP адрес е бил извлечен
- Кои крайни точки и системи да бъдат спрени, за да се предотвратят последващи зловредни процеси от атаките

ВАНИЯ НА ENDPOINT SECURITY

dpoint Security изисква 1 Ghz или по-висок Pentium съвместим процесор и поне 300 MB свободно дисково пространство. Работи със следните операционни системи:

ОПЕРАЦИОННА СИСТЕМА	МИНИМАЛНА ПАМЕТ НА СИСТЕМАТА (RAM)
Windows XP SP3	512 MB
Windows 2003 SP2	512 MB
Windows Vista SP1 или по-нова версия	1 GB (32-bit), 2 GB (64-bit)
Windows 2008 R2	2 GB (64-bit)
Windows 7	1 GB (32-bit), 2 GB (64-bit)
Windows 2012 (включително R2)	2 GB (64-bit)
Windows 8	1 GB (32-bit), 2 GB (64-bit)
Windows 8.1	1 GB (32-bit), 2 GB (64-bit)
Windows 10	1 GB (32-bit), 2 GB (64-bit)

СПЕЦИФИКАЦИИ НА ХАРДУЕРНОТО УСТРОЙСТВО

За момента Endpoint Security изисква хардуерно устройство за комуникация и разузнаване на заплахите. Устройството, както е посочено по-долу,трябва да поддържа до 100k крайни точки.

СПЕЦИФИКАЦИЯ	HX 4402/HX 4400D
Капацитет на паметта	4x 1.8 TB HDD, RAID 10, 2.5 inch, FRU
Кутия	1RU, Fits 19 inch Rack
Размери на шасито (ШхДхВ)	17.2" x 27.8" x 1.7" (437 x 706 x 43.2 mm)
AC Power Supply	Redundant (1+1) 750 watt, 100 240 VAC
Максимална консумация на енергия (вата)	313вата
MTBF (h)	35,200 h
Само устройството	32 lb. (15 kg)

За повече информация относно FireEye, посетете:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

© 2016 FireEye, Inc. Всички права запазени. FireEye е регистрирана търговска марка на FireEye, Inc. Всички други марки, продукти или услуги са или могат да бъдат търговски марки или марки на ус на съответните им собственици. DS.EPS.EN-US.022016

FireEye

Подписаната, [redacted], ЕГН: [redacted], Потвърждение №: 18ПР-1398/26.02.2018 г., удостоверявам верността на превода от английски на български език на приложения документ –, извършен от мен. Преводът се състои от 4 страници.

Подпис: [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

ENDPOINT SECURITY

DETECT AND PROTECT AGAINST UNKNOWN ENDPOINT THREATS AND EXPLOITS WITH INTEGRATED THREAT INTELLIGENCE

With FireEye Endpoint Security (HX series), organizations can proactively inspect, analyze and contain known and unknown threats at any endpoint.

HIGHLIGHTS

- Extend integrated FireEye Threat Intelligence from core to endpoint for comprehensive protection against advanced threats
- Conduct detailed endpoint investigations to identify and contain IOCs and create event timelines with Triage Viewer
- Detect, identify and contain threats on tens of thousands of endpoints (connected or not) in minutes via Enterprise Security Search
- Easily assess endpoint activities to identify exploits and alert analysts
- Comply with both Common Criteria and FIPS government standards
- Centralize host-based workflows with a single location for current alerts, system details and acquisitions
- Respond rapidly to known and unknown threats with critical contextual information
- Protect all endpoints whether on- or off-premise, outside the network, or behind network address translation (NAT)
- Contain threats and compromised devices with a single click while still allowing for remote investigation

Today's skilled attackers bypass traditional defenses most security teams have relied on for years to protect their endpoints. Even when a traditional defense stops a known threat, it can't determine what that threat was trying to do. FireEye Endpoint Security helps your security team hunt down and stop known and unknown advanced threats against your endpoints using features such as:

- Triage Viewer to view known indicators of compromise (IOCs)
- Enterprise Security Search to rapidly scan for and contain threats
- Data Acquisition for in-depth endpoint inspection and analysis
- Exploit Guard, which relies on years of threat intelligence, to detect exploit processes on endpoints

ВЯРНО С ОРИГИНАЛА

FireEye
SECURITY REIMAGINED

EXTEND THREAT INTELLIGENCE TO EVERY ENDPOINT

To be effective, threat intelligence must be present at the point of attack. Endpoint Security seamlessly extends the threat intelligence capabilities of other FireEye products to the endpoint. If a FireEye product detects an attack anywhere in the network, endpoints are automatically updated and inspected for IOCs.

ATTAIN ENHANCED ENDPOINT VISIBILITY

Visibility is critical to identifying the root cause of an alert and enables you to conduct deep analyses of the threat. The lookback cache in Endpoint Security allows you to inspect and analyze present and past network alerts (including those from a SIEM) at the endpoint. Triage Viewer provides you with an automatically collected timeline of events for any endpoint.

DETECT HIDDEN ENDPOINT EXPLOIT PROCESSES

Endpoint exploits challenge traditional Endpoint Protection (EPP) capabilities that focus on a single activity from a single endpoint. Exploit Guard is a data-driven flexible exploit intelligence feature that delivers Endpoint Detection and Response (EDR) capabilities and protects against the attacks traditional endpoint solutions miss. Using a decade's worth of exploit intelligence from the FireEye MVX engine, the Exploit Guard feature enables tthe Exploit Guard feature enables the HX series to assess multiple seemingly disparate activities across one or more endpoints to determine if an exploit is taking place.

GET COMPLETE ENDPOINT COVERAGE

On-site and remote endpoints outside the corporate network are key vulnerabilities. Endpoint Security covers all endpoints, pushing intelligence on IOCs to them regardless of Internet connection type. This enables you to investigate and contain endpoints anywhere in the world, without requiring additional VPN connections.

CONTAIN COMPROMISED ENDPOINTS AND PREVENT LATERAL SPREAD

Attacks that start at an endpoint can spread quickly through your network. After you identify an attack, Endpoint Security lets you immediately isolate compromised devices to stop the attack and prevent lateral spread—all with a single click. You can then conduct a complete forensic investigation of the incident without risking further infection.

HOW ENDPOINT SECURITY WORKS

FireEye Endpoint Security uses threat intelligence to correlate alerts generated by FireEye network platforms, log management, and network security products with IOCs on any endpoint. Once a threat has been validated, Endpoint Security can investigate tens of thousands of endpoints in minutes, and isolate compromised endpoints with a single click while you assess further potential risks.

With Endpoint Security you can figure out:

- Which vectors an attack used to infiltrate your system
- If the attack spread laterally to other systems
- If an attack occurred on a specific endpoint and whether it persists
- How long an endpoint(s) has been compromised
- If IP has been exfiltrated
- Which endpoints and systems to contain to prevent further compromise

ВЯРНО С ОРИГИНАЛА

ENDPOINT SECURITY REQUIREMENTS

Endpoint Security requires a 1 Ghz or higher Pentium compatible processor and at least 300 MB of free disk space. It works with the following operating systems:

OPERATING SYSTEM	MINIMUM SYSTEM MEMORY (RAM)
Windows XP SP3	512 MB
Windows 2003 SP2	512 MB
Windows Vista SP1 or newer	1 GB (32-bit), 2 GB (64-bit)
Windows 2008 R2	2 GB (64-bit)
Windows 7	1 GB (32-bit), 2 GB (64-bit)
Windows 2012 (including R2)	2 GB (64-bit)
Windows 8	1 GB (32-bit), 2 GB (64-bit)
Windows 8.1	1 GB (32-bit), 2 GB (64-bit)
Windows 10	1 GB (32-bit), 2 GB (64-bit)

HARDWARE APPLIANCE SPECIFICATIONS

Endpoint Security currently requires a hardware appliance for communication and threat intelligence. An appliance, as specified below, supports up to 100k endpoints.

SPECIFICATION	HX 4402/HX 4400D
Storage Capacity	4x 1.8 TB HDD, RAID 10, 2.5 inch, FRU
Enclosure	1RU, Fits 19 inch Rack
Chassis Dimensions (WxDxH)	17.2" x 27.8" x 1.7" (437 x 706 x 43.2 mm)
AC Power Supply	Redundant (1+1) 750 watt, 100 - 240 VAC
Power Consumption Maximum (watts)	313 watts
MTBF (h)	35,200 h
Appliance Alone	32 lb. (15 kg)

For more information on FireEye, visit:
www.FireEye.com

ВЯРНО С ОРИГИНАЛА

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

© 2016 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. DS.EPS.EN-US.022016

FireEye

Stiliyana Mahaldjiiska
FIREEYE™ L&S
TRANSLATION OFFICE

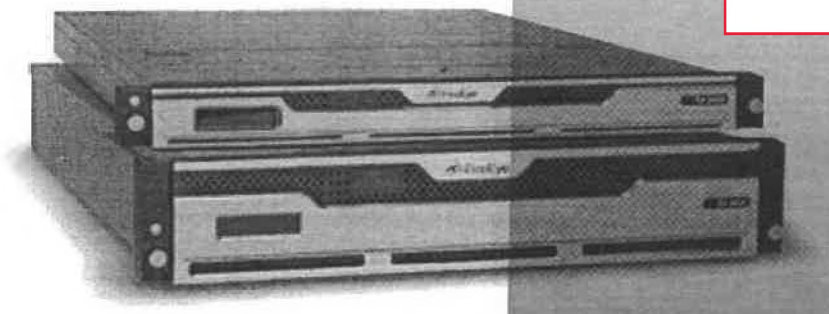
Продуктова брошура

FireEye Central Management

Централизирайте управлението на устройството и разузнаването, за да съпоставите данните между векторите на атаката

АКЦЕНТИ

- **Предлага интегрирани контроли за множество внедрявания на платформата**
- **Осигурява смесено предотвратяване на заплахи чрез многовекторна корелация**
- **Осигурява целенасочена платформа, която може да бъде внедрена за по-малко от 60 минути**
- **Използва лесно за разбиране табло за сигурност, което осигурява усъвършенстван статус на защитата срещу атаки**
- **Ускорява отчети и одити през консолидиран склад за събития свързани със сигурността**
- **Опростява управлението на множество решения на FireEye и намалява времето, прекарано в управление на конфигурации, актуализации на заплахи и надстройки на софтуера**



Фигура 1. CM 4500 и CM 9500 (не е изобразен CM 7500).

Общо представяне
FireEye® Central Management (серия CM) консолидира администрирането, отчитането и споделянето на данни от продуктите на FireEye в едно лесно за внедряване мрежово решение. Централното управление позволява споделяне в реално време на автоматично генерирана информация за заплахите с цел идентифициране и блокиране на напреднали атаки, насочени към Вашата организация. Също така дава възможност за централизирано конфигуриране, управление и отчитане на решенията на FireEye.

Споделяне в реално време на информация за локална заплаха
Решенията на FireEye генерират разузнавателна информация за заплахите в реално време, използвайки FireEye Multi-Vector Virtual Execution™ (MVX). Централното управление разпространява тази информация за заплахи към множество внедрени FireEye във Вашите системи, като гарантира, че всяко решение има еднакви динамични защити срещу напредналите атаки. Абонатите на облака FireEye Dynamic Threat Intelligence ™ (DTI) могат да използват централното управление, за да централизират изпращането и получаването на анонимно разузнаване на заплахите в FireEye решения, разположени при клиенти, технологични партньори и доставчици на услуги по целия свят.

Лесно за разбиране табло за сигурност плюс подробни разбивки
Централното управление консолидира дейностите и подобрява информираността за ситуацията чрез единно табло за сигурност. Таблото за управление дава на администраторите изглед в реално време на броя на заразените системи и директно се насочва към подробности за заразяването, за да се определят следващите стъпки.

0002448

ЕТ „Л и С - Стилияна Махалджийска“
Офис „Изток“: 1113 София, ул. Жолио Кюри 46Б, тел./факс: 02 963 44 04
Офис „Младост 1“: 1784 София, бул. Йерусалим, бл. 54, офис 11, партер (в двора ... 74 57 55
Офис „Бизнес парк София“: 1715 София, Бизнес парк София, сграда 8, вх. А - Б, те...
ЕТ „L&S - Stiliyana Mahaldjiiska“
Office „Istok“: 1113 Sofia Bulgaria, 46B, Fr. J. Curie Str., tel./fax: 02 963 44 04
Office „Mladost 1“: 1784 Sofia Bulgaria, 54, Yerusalim Blvd., Office 11, ground floor, tel./fax: 02 974 57 55
Office „Business Park Sofia“: 1715 Sofia Bulgaria, Business Park Sofia, building 8, ent. A-B, tel.: +359 2 489 81 55

office@variante.info
sliai@abv.bg
+359 888 875 932
www.variante.info

...диран анализ на напреднали целенасочени атаки
...а възможен анализът на смесени заплахи, като например ...криване на фишинг имейл атака, чиито съобщения целят разпространение на злонамерени URL адреси, като се извършва корелация на алармите с алармите от крайните точки, за проследяване на инцидента. Анализаторите на сигурността могат да свържат точките от смесена атака, за да получат необходимата информация, за да защитят своята организация срещу напреднали целенасочени атаки.

Корпоративен клас конзола и алармиране
Централното управление предоставя уеб-базирана GUI конзола, в която събития могат да се видят, търсят и филтрират и могат да се изпращат известия за сигнали в реално време чрез SMTP, SNMP, syslog или HTTP POST. Администраторите могат да филтрират по събития, дати или IP диапазони като се визуализиратрезултати само за да показват данни въз основа на оперативната роля на администратора в ИТ.
Известията могат да се изпращат и на SIEM инструменти на трети страни. Администраторите могат да натиснат върху връзка за събитие и да се свържат безпроблемно към конкретни решения на FireEye, за да видят защитен мрежов сегмент.

Централна конфигурация и обновяване на платформата
За ефективно внедряване в организацията, Централното управление разполага с динамични конфигурации. Настройките могат да бъдат определени централно и след това съответно да бъдат разпределени в една организация. Администраторите могат дистанционно да конфигурират и преглеждат настройки за едно или повече решения за защита на FireEye. Плюс това, всички обновления на софтуера могат да бъдат едновременно внедрени във всички управлявани решения, като по този начин се гарантира, че всички те имат най-новите възможности за сигурност.

Консолидиран склад и подробно отчитане По-големите и регулирани организации могат да използват Централното управление за ефективно, консолидирано отчитане на данни за сигурността. Централното управление Ви позволява да събирате и съхранявате свързани с одита събития за сигурност, за да отговаряте на дългосрочните изисквания за запазване на данните.

Централното управление предлага удобни начини за търсене и докладване на заплахи по име или тип. Организациите могат също така да получават обобщения като например такива за най-заразените хостове и вирусен софтуер и събития за обратно извикване, включително данни за геолокация. Статистическите изгледи могат да помогнат да се покаже напредъкът към намаляване на броя на компрометираните системи.

Таблица 1. Спецификации на устройството.

	CM 4500	CM 7500	CM 9500
Портове на мрежов интерфейс	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
Портове за управление (заден панел)	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
IPMI Порт (заден панел)	Включен	Включен	Включен
LCD и клавиатура на предния панел	Включени	Включени	Включени
PS / 2 клавиатура и мишка, DB15 VGA портове (заден панел)	Включени	Включени	Включени
USB портове (заден панел)	2x Type A USB Ports	2x Type A USB Ports	2x Type A USB Ports
...иен порт (заден панел)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Капацитет на съхранение	4x 4 TB HDD, RAID 10 Usable; 8TB	4x 4 TB HDD, RAID 10 Usable; 8TB	4x 4 TB HDD, RAID 10 Usable; 8TB
Кутия	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Размери на шасито (ШхДхВ)	17.2"x 25.6" x 1.7" (437 x 650 x 43.2 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)
Захранване	Redundant (1+1) 750W AC PSUs	Redundant (1+1) 800W AC PSUs	Redundant (1+1) 800W AC PSUs
Максимална консумация на енергия (вата)	245 вата	456 вата	612 вата
Максимално излъчване на топлина (BTU/h)	836 BTU/h	1556 BTU/h	2088 BTU/h
MTBF (h)	35,200 h	60,700 h	60,700 h
Тегло само на устройството / на доставения пакет lb. (kg)	30.0 lbs (13.6Kg) / 41.0 (18.6Kg)	44.1 lbs (20.0 kg) / 65.3 lbs (29.6 kg)	50.4 lbs (22.9 Kg) / 71.6 lbs (32.5 Kg)

Забележка: Всички стойности на производителността варират в зависимост от системната конфигурация и профила на трафика, който се обработва.

ЕТ "L&S - St. Mahaldjiiska" * Sofia L&S София * ЕТ "ПиС - Ст. Махалджийска"

аблица 1. Спецификации на устройството.

	CM 4500	CM 7500	CM 9500
Сертификати за сигурност	IEC 60950, EN 60950, CSA 60950-00, CE Marking	IEC 60950, EN 60950, CSA 60950-00, CE Marking	IEC 60950, EN 60950, CSA 60950-00, CE Marking
EMC/EMI Сертификати	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A
Съответствие с нормативната уредба	RoHS, REACH, WEEE	RoHS, REACH, WEEE	RoHS, REACH, WEEE
Работна температура	0 ~ 35° C	0 ~ 35° C	0 ~ 35° C
Работна относителна влажност	10 ~ 95% @ 40° C, без кондензация	10 ~ 95% @ 40° C, без кондензация	10 ~ 95% @ 40° C, без кондензация
Работна височина	5,000 ft.	5,000 ft.	5,000 ft.

Забележка: Всички стойности на производителността варират в зависимост от системната конфигурация и профила на трафика, който се обработва.

блица 2. Спецификации на виртуалното устройство.

Модел	CPU ядра	RAM	Виртуални NICS	Капацитет на твърдия диск
CM2500V	4	32 GB	4 (общо): 1 (за управление) 1-3 (за употреба в бъдеще)	512 GB
CM7500V	16	128 GB	4 (общо): 1 (за управление) 1-3 (за употреба в бъдеще)	1200 GB

Забележка: Всеко виртуално устройство трябва да отговаря на тези спецификации.

За да научите повече за FireEye, посетете: www.FireEye.com

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2019 FireEye, Inc. Всички права запазени. FireEye е регистрирана търговска марка на FireEye, Inc. Всички други марки, продукти или услуги са или могат да бъдат търговски марки или марки на услуги на съответните им собственици. NS-EXT-DS-US-EN-000191-01

За FireEye, Inc.
FireEye е компания за интелигентна охрана. Работейки като безпроблемно, мащабируемо разширение на защитните операции на клиентите, FireEye предлага единна платформа, която съчетава иновативни технологии за сигурност, информация заплахи на национално ниво и световно призната консултация Mandiant®. С този подход FireEye елиминира сложността и тежестта на киберсигурността за организации, които се борят да се подготвят, предотвратяват и реагират на кибератаки.

FIREEYE

ЕТ "ЛиС - Ст. Махалджийско"

Подписаната, [redacted], ЕГН: [redacted] Потвърждение №: 18ПР-1398/26.02.2018 г., удостоверявам верността на превода от английски на български език на приложения документ –, извършен от мен. Преводът се състои от 4 страници.

Подпис: [redacted]

ЕТ "ЛиС - Ст. Мавалджийска" * ЕТ "ЛиС - St. Mahaldjiiska" * Sofia

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

FIREEYE™

DATA SHEET

FireEye Central Management

Centralize device and intelligence management to correlate data across attack vectors

HIGHLIGHTS

- Offers integrated controls for multiple platform deployments
- Enables blended threat prevention through multi-vector correlation
- Provides a purpose-built platform that can be deployed in less than 60 minutes
- Displays an at-a-glance security dashboard that provides advanced targeted attack protection status
- Speeds reports and audits through a consolidated security event storehouse
- Streamlines management of multiple FireEye solutions and reduces time spent managing configurations, threat updates and software upgrades

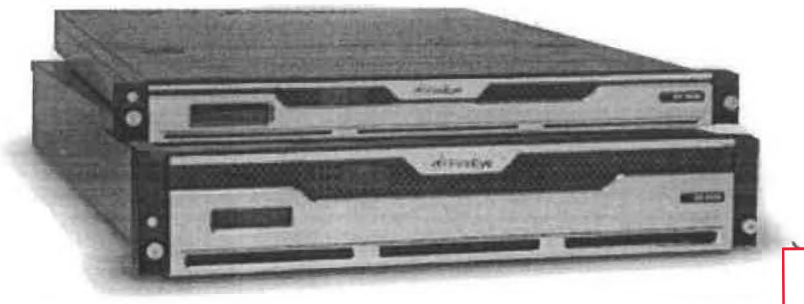


Figure 1. CM 4500 and CM 9500 (not pictured CM 7500).

Overview

FireEye® Central Management (CM series) consolidates the administration, reporting and data sharing of the FireEye products in one easy-to-deploy, network-based solution. Central Management enables real-time sharing of auto-generated threat intelligence to identify and block advanced attacks targeting your organization. It also enables centralized configuration, management and reporting of FireEye solutions.

Real-time sharing of local threat intelligence

FireEye solutions generate real-time threat intelligence using the FireEye Multi-Vector Virtual Execution™ (MVX) engine. Central Management distributes that threat intelligence to multiple FireEye deployments across your systems, ensuring that each solution has the same dynamic protections against the advanced attacks. Subscribers to the FireEye Dynamic Threat Intelligence™ (DTI) cloud can use the Central Management to centralize the sending and receiving of anonymized threat intelligence across FireEye solutions deployed at customers, technology partners and service providers around the world.

At-a-glance security dashboard, plus drilldowns

Central Management consolidates activities and improves situational awareness with a unified security dashboard. The dashboard gives administrators a real-time view of the number of infected systems and drill directly down to infection details to determine next steps.

ВЯРНО С ОРИГИНАЛА

Unified analysis of advanced targeted attacks
The analysis of blended threats, such as pinpointing a spear-phishing email used to distribute malicious URLs and correlating a perimeter alert to the endpoint, becomes possible. Security analysts can connect the dots of a blended attack, to get the actionable intelligence they need to protect their organization against advanced targeted attacks.

Enterprise-class console and alerting
Central Management provides a web-based GUI console in which events can be seen, searched and filtered and real-time alert notifications can be sent via SMTP, SNMP, syslog or HTTP POST. Administrators can filter by events, dates or IP ranges and results are displayed to only show data based on the administrator's IT operational role. Notifications can also be sent to third-party SIEM tools. Administrators can click on an event link and connect seamlessly to specific FireEye solutions to view the network segment being protected.

Central configuration and platform upgrades
For efficient enterprise deployments, Central Management features dynamic configurations. Settings can be determined centrally and then distributed across an organization accordingly. Administrators can remotely configure and view settings for a one or more FireEye security solutions. Plus, all upgrades can be simultaneously deployed to all managed solutions, ensuring that they all have the latest security capabilities.

Consolidated storehouse and detailed reporting
Larger and regulated organizations can use Central Management for efficient, consolidated reporting of security data. Central Management enables you to collect and store audit-relevant security events to meet long-term data retention requirements.

Central Management offers convenient ways to search for and report on threats by name or type. Organizations can also view summaries such as the top infected hosts and malware and callback events, including geolocation details. Trending views can help show progress toward reducing the number of compromised systems.

Table 1. Appliance specifications.

	CM 4500	CM 7500	CM 9500
Network Interface Ports	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
Management Ports (rear panel)	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
IPMI Port (rear panel)	Included	Included	Included
Front Panel LCD & Keypad	Included	Included	Included
PS/2 Keyboard and Mouse, DB15 VGA Ports (rear panel)	Included	Included	Included
USB Ports (rear panel)	2x Type A USB Ports	2x Type A USB Ports	2x Type A USB Ports
Serial Port (rear panel)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Storage Capacity	4x 4 TB HDD, RAID 10 Usable; 8TB	4x 4 TB HDD, RAID 10 Usable; 8TB	4x 4 TB HDD, RAID 10 Usable; 8TB
Enclosure	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Chassis Dimensions (WxDxH)	17.2"x 25.6" x 1.7" (437 x 650 x 43.2 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)
AC Power Supply	Redundant (1+1) 750W AC PSUs	Redundant (1+1) 800W AC PSUs	Redundant (1+1) 800W AC PSUs
Power Consumption Maximum (watts)	245 watts	456 watts	612 watts
Thermal Dissipation Maximum (BTU/h)	836 BTU/h	1556 BTU/h	2088 BTU/h
MTBF (h)	35,200 h	60,700 h	60,700 h
Appliance Alone / As Shipped Weight lb. (kg)	30.0 lbs (13.6Kg) / 41.0 (18.6Kg)	44.1 lbs (20.0 kg) / 65.3 lbs (29.6 kg)	50.4 lbs (22.9 Kg) / 71.6 lbs (32 Kg)

Note: All performance values vary depending on the system configuration and traffic profile being processed.

ВЯРНО С ОРИГИНАЛА

Table 1. Appliance specifications.

	CM 4500	CM 7500	CM 9500
Safety Certifications	IEC 60950, EN 60950, CSA 60950-00, CE Marking	IEC 60950, EN 60950, CSA 60950-00, CE Marking	IEC 60950, EN 60950, CSA 60950-00, CE Marking
EMC/EMI Certifications	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A
Regulatory Compliance	RoHS, REACH, WEEE	RoHS, REACH, WEEE	RoHS, REACH, WEEE
Operating Temperature	0 - 35° C	0 - 35° C	0 - 35° C
Operating Relative Humidity	10 - 95% @ 40° C, non-condensing	10 - 95% @ 40° C, non-condensing	10 - 95% @ 40° C, non-condensing
Operating Altitude	5,000 ft.	5,000 ft.	5,000 ft.

Note: All performance values vary depending on the system configuration and traffic profile being processed.

Table 2. Virtual appliance specifications.

Model	CPU Cores	RAM	Virtual NICS	Hard Disk Space
CM2500V	4	32 GB	4 (total): 1 (management) 1-3 (for future use)	512 GB
CM7500V	16	128 GB	4 (total): 1 (management) 1-3 (for future use)	1200 GB

Note: Each virtual appliance must meet the following specifications.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. NS-EXT-DS-US-EN-000191-01

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™

ВЯРНО С ОРИГИНАЛА

ET „Л и С - Стилияна Махалджийска“
Офис „Изток“: 1413 София, ул. „Цоколо Кюрт“ 46б; тел./факс: 02 963 44 04
Офис „Младост 1“: 1784 София, бул. „Йерусалим“ бл. 54, офис 9; тел./факс: 02 974 57 55
Офис „Бизнес парк София“: 1715 София, „Бизнес парк София“, сграда 8, ет. А-В; тел.: +359 2 489 81 55
ET „L&S - Stiliyana Mahaldjiska“
Office „Istok“: 1113 Sofia, Bulgaria, 46B, Fr. J. Curie Str., tel./fax: 02 963 44 04
Office „Mladost 1“: 1784 Sofia, Bulgaria, 54, Yerusalim Blvd., Office 11, ground floor; tel./fax: 02 974 57 55
Office „Business Park Sofia“: 1715 Sofia Bulgaria, Business Park Sofia, building 8, ent. A-B, tel.: +359 2 489 81 55

Stiliyana Mahaldjiska
L&S - STILIYANA MAHALDJIISKA OFFICE

FIREEYE™

Продуктова брошура

FireEye Network Security

Ефективна защита срещу пробиви в киберсигурността на средни и големи организации

Общо представяне

FireEye Network Security е ефективно решение за киберзащита, което помага на организациите да намалят до минимум риска от пробиви в сигурността, водещи до големи загуби, чрез безпогрешно откриване и незабавно спиране на напреднали, целенасочени и други скрити атаки, намиращи се в интернет трафика. То улеснява ефективното разрешаване на открити проблеми със сигурността за броени минути, предоставяйки конкретни доказателства, активно разследване и интегриране в работния процес по отстраняването на възникнали заплахи. С FireEye Network Security организациите са ефективно защитени срещу днешните заплахи, независимо дали те са насочени към операционните системи Microsoft Windows, Apple OS X или уязвими приложения; към централата или клоновете на организацията; или са скрити в голям обем входящ интернет трафик, който трябва да бъде инспектиран в реално време.

В основата на FireEye Network Security са технологиите Multi-Vector Virtual Execution ™ (MVX) и Intelligence-Driven-Analysis (IDA).

MVX е динамична технология без използване на дефиниции, който проверява подозрителен мрежов трафик, за да идентифицира атаки, които избягват традиционните защити, базирани на дефиниции и политики. IDA е съвкупност от контекстуални технологии с динамични правила, които откриват и блокират вируси в реално време и със задна дата, на базата на най-новата информация за таргетирани машини, нападатели и жертви. FireEye Network Security също така включва и технология за предотвратяване на проникванія (IPS) за откриване на често срещани атаки, използвайки конвенционалното сравнение на дефиниции по списък.

FireEye Network Security се предлага в различни конфигурации, възможности за внедряване и производителност. Обикновено се поставя на пътя на интернет трафика зад традиционните устройства за мрежова сигурност като защитни стени от ново поколение, IPS и решения за защита на уеб трафик на ниво gateway (SWG). FireEye Network Security допълва тези решения като бързо открива както познати, така и неизвестни атаки с висока точност и ниска степен на грешни положителни резултати, като същевременно предоставя ефективен отговор на всяка вдигната аларма.

Фигура 1. Обичайна конфигурация — Решения за мрежова сигурност FireEye Network Security.

00022451

office@variante.info
sliai@abv.bg
+359 888 875 932
www.variante.info

Прецизно откриване на напреднали, целенасочени и други скрити кибератаки	Минимизира риска от кибер-атаки водещи до финансови загуби
Разширяема, модулна архитектура за защита	Осигурява защита на инвестициите
Постоянно ниво на защита за среди с разнородни операционни системи и за всички точки за достъп до Интернет	Създава силна защита в цялата организация за всички видове устройства
Интегрирани, разпределени, физически, виртуални, локални и облачни възможности за внедряване	Предоставя гъвкавост за привеждане в съответствие с организационните предпочитания и ресурси
Многовекторна корелация с решения за защита на електронна поща и решения за защита на съдържанието	Осигурява видимост над множество вектори на атака
Предотвратяване	
Незабавно блокиране на атаки при скорости на мрежата от 10 Mbps до 8 Gbps	Осигурява защита в реално време срещу скрити атаки
Отговор	
Нисък процент на грешни показания, категоризация на рисков софтуер и автоматизирано валидиране на алармите от IPS	Намалява оперативните разходи за обработване на ненадеждни сигнали
Проверка и валидиране на аларми, ограничаване на крайната точка и реакция при инциденти	Автоматизира и опростява работните процеси свързани със сигурността
Доказателства за изпълнение на зловреден код и активно разузнаване на заплахи с контекстуална информация	Ускорява приоритизирането и разрешаването на открити проблеми със сигурността
Възможност за надграждане от един до хиляди обекти	Възможност за разширяване с растежа на бизнеса

...ски предимства

Безпогрешно откриване на заплахи

FireEye Network Security използва множество техники за анализ за откриване на атаки с висока точност и ниска степен на грешни показания:

- Multi-Vector Virtual Execution ™ (MVX) технологията открива непознати, многопоточни и други скрити атаки чрез динамичен анализ без използване на дефиниции в безопасна, виртуална среда. Спират се фазите на заразяване и компрометиране от етапите на изпълнение на кибер-атаките чрез идентифициране на напълно непознат вирусен софтуер.
- Intelligence-Driven Analysis (IDA) софтуерите, откриват и блокират скрити, целенасочени и други персонализирани атаки с контекстуален, базиран на правила анализ на информация в реално време, събрана на първа линия от милиони MVX случаи, хиляди часове опит от реакция на инциденти получен от Mandiant, компания на FireEye, и стотици изследователи на заплахи iSight. Той спира фазите на заразяване, компрометиране и проникване от етапите на изпълнение на кибер-атаките чрез идентифициране на злонамерени експлоатации, вирусен софтуер и отговори на команди и контрол (CnC). Той също так извлича и изпраща подозрителен мрежов трафик на MVX софтуера за окончателен анализ случая.
- Structured Threat Intelligence eXpression (STIX) позволява получаването на информация за заплахи от трети страникато използва формат с индустриален стандарт за добавяне на персонализирани индикатори за заплаха в IDA софтуера.

Незабавна и устойчива защита

FireEye Network Security предлага гъвкави конфигурационни режими, включително:

- Мониторинг извън мрежата чрез TAP / SPAN, вграден мониторинг или активно блокиране на вградени данни. Режимът на блокиране на вградени данни автоматично блокира входящи експлоатации и вирусен софтуер и изходящите мулти-протоколни обратни повиквания. В режима на вътрешен мониторинг се генерират сигнали като организациите решават как да отговорят на тях. В режим на превенция извън мрежата FireEye Network Security издава TCP за повторно блокиране извън мрежата на TCP, UDP или HTTP връзки.
- Избраните модели предлагат активна опция с висока наличност (HA) с цел осигуряване на устойчивост в случай на повреда в мрежата или устройството.

Защита на множество вектори за атаки

FireEye Network Security осигурява постоянно ниво на защита за разнообразните мрежови среди:

- Поддръжка на най-често срещаните операционни системи Microsoft Windows и Apple Mac OS X
- Анализ на над 140 различни типа файлове, включително преносими изпълними файлове (PE), уеб съдържание, архиви, изображения, Java, Microsoft и Adobe приложения и мултимедия
- Изпълнение на подозрителен мрежов трафик срещу хиляди операционни системи, service pack версии, типове приложения и комбинации от техните версии
- Защита срещу модерни атаки и видове вирусен софтуер, които трудно могат да бъдат открити чрез дефиниции: уеб качвания, уеб изпълнение, ransomware, cryptominers

Валидирани и приоритетни сигнали

В допълнение към откриването на истински атак технологията FireEye MVX се използва и за определяне на надеждността на сигналите, откри чрез конвенционалните методи за съчетание на дефиниции и за идентифициране и определяне н приоритета на критични заплахи:

- Системата за предотвратяване на проникванияя (IPS) със софтуера за валидиране MVX намалява времето, необходимо за разпознаване на базата на дефиниции, което традиционно е предразположено към фалшиви сигнали
- Категоризирането на рисковия софтуер разделя истинските опити за нарушение от нежеланата, но по-малко злонамерена дейност (като рекламен и шпионски софтуер), за да се приоритизира сигнала, на който да се отговори

ЕТ "L&S - St. Mahaldjiiska" Sofia L&S София ЕТ "ЛиС - Ст. Махалджийска"

Активна информация за заплахи
Сигналите, генерирани от FireEye Network Security, включват конкретни доказателства и контекстуална информация за бързо реагиране, приоритизиране и спиране на заплаха:

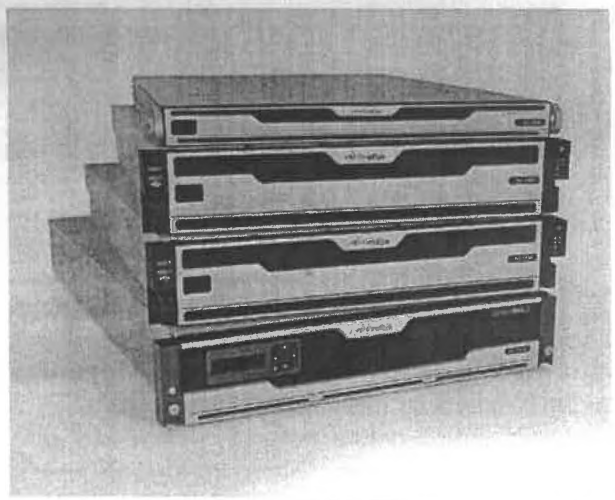
- Dynamic Threat Intelligence (DTI): конкретни, споделяни в реално време данни в глобален мащаб за бързо и проактивно спиране на целенасочени и новооткрити атаки
- Advanced Threat Intelligence (ATI): контекстуална информация за атаката с цел ускоряване на реакцията и предписателни указания за ограничаване на заплахата

Интеграция на работния поток за реакция
FireEye Network Security може да бъде разширен по няколко начина, за да се автоматизират работните потоци за отговор на сигналите:

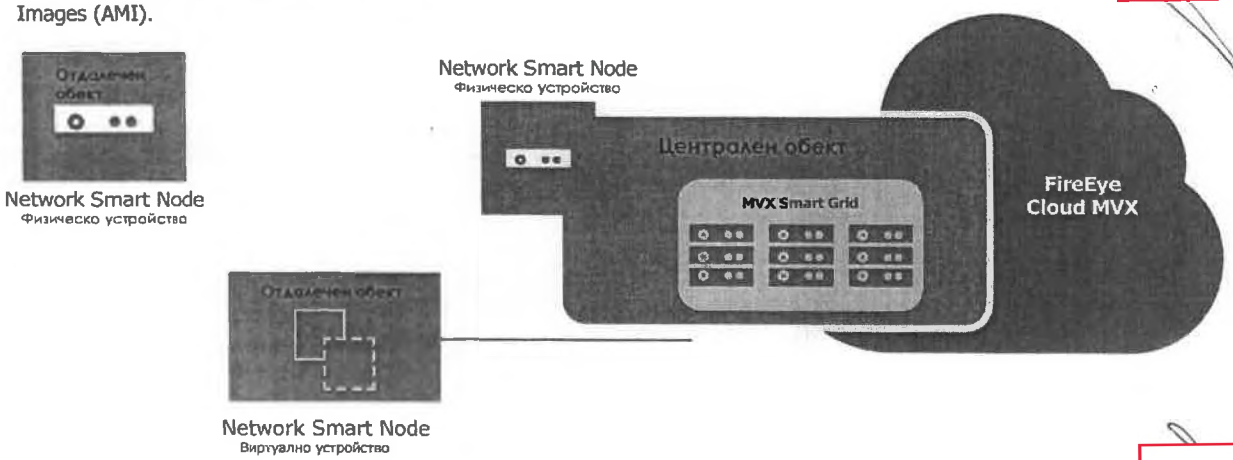
- FireEye Central Management корелира сигналите както от FireEye Network Security, така и от FireEye Email Security с цел по-широк поглед върху атаката и задаване на правила за блокиране, които не позволяват на атаката да се разпространи
- FireEye Network Forensics се интегрира с FireEye Network Security, за да предостави подробни пакетни проучвания на сигнал и да даде възможност за задълбочени разследвания
- FireEye Endpoint Security идентифицира, валидира и спира компромиси, открити от FireEye Network Security за опростяване на ограничаването и отстраняването на засегнатите крайни точки

Опции за гъвкаво внедряване
FireEye Network Security предлага различни опции за внедряване, за да съответства на нуждите и бюджета на организацията:

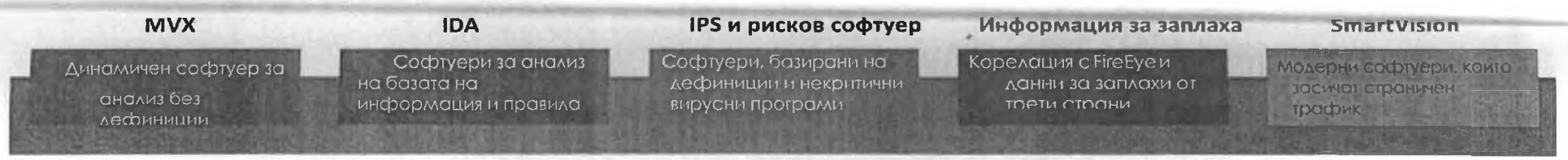
- Integrated Network Security: самостоятелно, многофункционално хардуерно устройство с интегрирана MVX услуга за осигуряване на точка за достъп до Интернет от един обект. FireEye Network Security е лесна за управление платформа без клиент, която се инсталира за по-малко от 60 минути. Не изисква правила, политики или настройка.
- Разпределена мрежова сигурност: разширяеми устройства с централно споделена MVX услуга за осигуряване на точки за достъп до Интернет в рамките на организациите
  - Network Smart Node: физически или виртуални устройства, които анализират интернет трафик, за да открият и блокират вирусен трафик и да подадат подозрителна активност през криптирана връзка към MVX услугата за окончателен анализ на случая
  - MVX Smart Grid: локална, централно разположена, еластична MVX услуга, която предлага прозрачна мащабируемост, вградено N + 1 отклонение и автоматизирано балансиране на натоварването
  - FireEye Cloud MVX: Хостван от FireEye абонамент за MVX услуга, който гарантира поверителност чрез анализ на трафика в Network Smart Node. Само съмнителни обекти се изпращат през криптирана връзка към MVX услугата, като не се разглеждат обекти за анализ, определени като доброкачествени.
  - Защита на място или в облака: Освен самостоятелни и виртуални устройства, FireEye предлага мрежова сигурност в публичния облак чрез Amazon Machine Images (AMI).



Фигура 2 Примерите за интегрирана мрежова сигурност включват NX 2550, NX 3500, NX 5500, NX 10550.



Фигура 3. Модели за внедряване на Network Security.



фигура 4. Модулни компоненти на FireEye Network Security.

Висока производителност и мащабируемост
FireEye Network Security защитава точките за достъп до Интернет в мрежата, като се предлага в различни варианти с различна производителност, за голям набор от размери на офиси и брой клонове на офиси:

Мащабируемата архитектура на MVX Smart Grid и FireEye Cloud MVX позволява на MVX услугата да поддържа от един Network Smart Node до хиляди и безпроблемно мащабиране при необходимост.

Формат	Работа
Интегрирана мрежова сигурност	50 Mbps до 5 Gbps
Физически Network Smart Node	50 Mbps до 10 Gbps
Виртуален Network Smart Node и Network Smart Node в публичен облак	50 Mbps до 1 Gbps

Ползи за бизнеса
Създаден, за да отговори на нуждите на организации с един обект и такива разпределени в много обекти, FireEye Network Security предоставя няколко предимства:

Минимизира риска от кибер-атаки
FireEye Network Security е високоефективно решение за киберзащита, което:

- Предотвратява външни лица да влязат в организацията, за да откраднат ценни активи или да нарушат бизнес процесите, като спира модерни, целенасочени и други скрити атаки
- Спира атаките и задържа прониквания по-бързо с конкретни доказателства, действаща информация, блокиране на вградени данни и автоматизация на работния процес
- Елиминира слабите места от кибер защитата на организацията с постоянна защита за различни операционни системи, типове приложения, клонове и централни обекти

Кратък срок на изплащане
Според скорошно проучване на Forrester Consulting[1], клиентите на FireEye Network Security може да очакват 152% спестявания от възвръщаемостта на инвестицията за период от три години изплащане на първоначалната инвестиция само за 9,7 месецаFireEye Network Security:

- Фокусира ресурсите на екипа за сигурност върху реални атаки с цел намаляване на оперативните разходи
- Оптимизира капиталовите разходи чрез споделена MVX услуга и голямо разнообразие от точки за ефективност с цел съразмерно внедряване, което да отговаря на изискванията
- Бъдещи инвестиции за сигурност чрез плавно мащабиране, когато броят на клоновете или количеството на интернет трафика нараства
- Защитава съществуващите инвестиции, като позволява безпроблемна миграция от интегрирано към разпределено внедряване
- Намалява бъдещите капиталови разходи чрез модулна и разширяваща се архитектура

Награди и сертификати
Продуктовото портфолио на FireEye Network Security е получило редица индустриални и правителствени награди и сертификати:

- През 2018 г. Frost & Sullivan признаха FireEye за безспорен пазарен лидер с 46% пазарен дял, повече от следващите десет конкурента взети заедно [2]
- FireEye Network Security е носител на множество награди от SANS Institute, SC Magazine, CRN и други
- FireEye Network Security беше първото решение за сигурност на пазара, което получи сертификат за безопасност на Министерството на вътрешната сигурност на САЩ

1 Forrester (May 2016). Общият икономически ефект от FireEye.

Таблица 1. FireEye Network Security спецификации, интегрирано устройство.

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Поддържани операционни системи	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Производителност *	До 50 Mbps или 100 Mbps	До 250 Mbps	До 500 Mbps	До 1 Gbps	До 2.5 Gbps	До 5 Gbps
Мрежови портове за мониторинг	4x 1GigE Bypass	4x 10GigE SFP+ 4x 1GigE Bypass	4x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 2x 40GigE QSFP+
Режим на работа на мрежовите портове	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) или TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) или TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) или TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) или TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) или TAP/SPAN	In-line, Monitor,TAP/SPAN
Висока наличност (HA)	Не е налична	Не е налична	Не е налична	Налична	Налична	Налична
Портове за управление (заден панел)	2x 10/100/1000 BASE- T Ports	2x 1GigE	2x 1GigE	2x 1GigE	2x 1GigE	2x 1GigE
IPMI порт	Преден панел	Заден панел	Заден панел	Заден панел	Заден панел	Заден панел
Преден LCD и клавиатура	Не са налични	Не са налични	Не са налични	Не са налични	Не са налични	Не са налични
VGA порт	Не	Да	Да	Да	Да	Да
USB портове	2x Type A USB портове(преден панел)	4x Type A USB портове (всички отзад)	4x Type A USB портове 2 отпред, 2 отзад	4x Type A USB портове 2 отпред, 2 отзад	4x Type A USB портове 2 отпред, 2 отзад	2x Type A USB портове
Сериен порт (заден панел)	115,200 bps, No Parity, 8 bits, 1 Stop Bit (RJ45 connector RJ45-to-Dsub включен е кабел за адаптер)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115200 bps, No Parity, 8 bits, 1 Stop Bit
Капацитет на диска	Single 1TB 3.5 inch, SATA HDD, вътрешен, фиксиран	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2x 10TB HDD 3.5", SAS3, 7.2krpm FRU RAID1
Кутия	1RU, Fits 19 inch Rack	1RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack	2RU, Fits 19 inch Rack
Размер на шасито ШхДхВ	17.2in(437mm) x 19.7in(500mm) x 1.7in(43.2 mm)	17.2in(437mm) x 25.6in(650mm) x 1.7in(43.2mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in (88.4mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in(88.4mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in(88.4mm)	17.2in(437mm) x 31.0in(787mm) x 3.5in(89mm)
Захранване	Single 250 watt, 90–264 VAC, 3.5–1.5 A, 50–60 Hz, IEC60320-C14, inlet, вътрешен, фиксиран	Redundant (1+1) 750 watt, 100–240 VAC 8.0–4.5A, 50–60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100–240 VAC 10.5–4.0A, 50–60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100–240 VAC 10.5–4.0A, 50–60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100–240 VAC 10.5–4.0A, 50–60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 1000 watt, 100–240 VAC 10.5–4.0A, 50–60 Hz IEC60320-C14 inlet, FRU

ЕТ "L&S - St. Mahadjijisk" Sofia L&S София ЕТ "ЛиС - Ст. Махалджийска"

Таблица 1. FireEye Network Security спецификации, интегрирано устройство. (продължение)

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Максимална консумация на енергия (вата)	85 вата	265 вата	426 вата	519 вата	658 вата	660 вата
Максимално излъчване на топлина (BTU/h)	290 BTU/h	904 BTU/h	1,454 BTU/hr	1,771 BTU/h	2,245 BTU/h	2,252 BTU/h
MTBF (h)	108,944 h	54,200 h	65,466 h	57,766 h	52,802 h	54,041 h
Тегло само на устройството / на доставения пакет lb. (kg)	16.2 lb (7.3 kg) / 28.2 lb (12.79 kg)	29.8 lbs (13.5 Kg) / 40.8 lbs (18.5 Kg)	37.4 lbs (17.0 Kg) / 58.6 lbs (26.6 kg)	42.4 lbs (19.2 Kg) / 63.5 lbs (28.8 kg)	42.7 lbs (19.2 Kg) / 63.8 lbs (29.0 kg)	44 lbs (20 kgs) 71 lbs (32.2Kg)
Безопасност в съответствие на нормативната уредба	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Сертификати за сигурност	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP vw1.1
ЕМС съответствие на нормативната уредба	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	Safety: EN 60950; C22.2; UL 60950; IEC 60950; CAN/ CSA-C22.2; K 60950 NZS 60950; GB 4943 J60950, SI60950 EMC: FCC Part 15 SubPart B Class A; ICES-003; EN55032; VCCI V-3; E 55024; EN 61000; CN 13438; CISPR32; KN32; KN 35
Съответствие с изискванията за опазване на околната среда	RoHS Directive 2011/65/ EU REACH WEEE Directive 2012/19/ EU	RoHS Directive 2011/65/ EU REACH WEEE Directive 2012/19/ EU	RoHS Directive 2011/65/ EU REACH WEEE Directive 2012/19/ EU	RoHS Directive 2011/65/ EU REACH WEEE Directive 2012/19/ EU	RoHS Directive 2011/65/ EU REACH WEEE Directive 2012/19/ EU	RoHS; REACH; WEEE Conflict Minerals
Работна температура	0–40°C 32–104°F	0–40°C 32–104°F	0–40°C 32–104°F	0–40°C 32–104°F	0–40°C 32–104°F	0–40°C 32–104°F
Температура в изключен режим	-20–80°C -4–176°F	-30–70°C -22–158°F	-40–70°C -40–158°F	-40–70°C -40–158°F	-40–70°C -40–158°F	-30–70°C -22–158°F
Работна относителна влажност	5–85% at 40°C без кондензация	10–95% @ 40° C, без кондензация	10–95% @ 40° C, без кондензация	10–95% @ 40° C, без кондензация	10–95% @ 40° C, без кондензация	10%–90%@40°C без кондензация
Относителна влажност в изключен режим	5–85% at 40°C без кондензация	10–95% @ 60° C, без кондензация	10–95% @ 60° C, без кондензация	10–95% @ 60° C, без кондензация	10–95% @ 60° C, без кондензация	10%–95%@55°C без кондензация
Работна височина	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft

[redacted]

[redacted]

[redacted]

[redacted]

ЕТ "Л&С - Ст. Махалджиева" София Л&С ЕТ "ЛиС - Ст. Махалджиева"

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Максимална работа на IPS	До 50 Mbps или 100 Mbps	До 250 Mbps	До 500 Mbps	До 1 Gbps	До 2.5 Gbps	До 5 Gbps
Максимални едновременни връзки	15K or 80K	80K	160K	500K	1M	2M
Нови свързвания за секунда	750/Sec or 4K/Sec	4K/Sec	8K/Sec	10K/Sec	20K/Sec	40K/Sec

Таблица 3. FireEye Network Security smart node, физически спецификации.

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Поддържани операционни системи	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Производителност	До 50 Mbps	До 100 Mbps or 250 Mbps	До 500 Mbps	До 1 Gbps	До 2 Gbps	До 5 Gbps	До 10Gbps
Мрежови портове за мониторинг	4x 10/100/1000 BASE-T портове	4x 1GigE Bypass	4x 10GigE SFP+ 4x 1GigE Bypass	4x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 2x 40GigE QSFP+
Режим на работа на мрежовите портове	In-line Monitor, Fail-Close или Tap	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) или TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) или TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) или TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) или TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) или TAP/SPAN	In-line, Monitor,T[illegible] SPAN
Висока наличност (HA)	Не е налична	Не е налична	Не е налична	Не е налична	Не е налична	Не е налична	Не е налична
Портове за управление (заден панел)	2x 10/100/1000 BASE- T портове	2x 1GigE	2x 1GigE	2x 1GigE	2x 1GigE	2x 1GigE	2x 1GigE
IPMI порт	Не е наличен	Преден панел	Заден панел	Заден панел	Заден панел	Заден панел	Заден панел
Преден LCD и клавиатура	Не са налични	Не са налични	Не са налични	Не са налични	Не са налични	Не са налични	Не са налични
VGA порт	Не е наличен	Не е наличен	Да	Да	Да	Да	Да
USB портове	2x Type A USB портове	2x Type A USB портове (преден панел)	4x Type A USB портове (всички отзад)	4x Type A USB портове 2 отпред, 2 отзад	4x Type A USB портове 2 отпред, 2 отзад	4x Type A USB портове 2 отпред, 2 отзад	2x Type A USB портове

ЕТ "L&S - St. Mabaldjitska" Sofia L&S София ЕТ"ТИС - Ст. Махалджийска"

Таблица 3. FireEye Network Security smart node, физически с

	NX 1500	NX 2500
Сериен порт (заден панел)	115,200 bps, No Parity, 8 bits, 1 Stop Bit (RJ45 connector; RJ45-to-Dsub включен е кабел за адаптер)	115,200 bps, No Parity, 8 bits, 1 Stop Bit (RJ45 connector RJ45-to-Dsub включен е кабел за адаптер)
Капацитет на диска	Single 500GB 2.5 inch SATA HDD, вътрешен, фиксиран	Single ITB 3.5 inch SATA HDD вътрешен, фиксиран
Кутия	Форматор за десктоп	1RU, Fits 19 inch Rack
Размер на шасито ШхДхВ	11in(280mm) x 6.9in(175mm) x 1.7in (44mm)	17.2in(437mm) x 19.7in(500mm) x 1.7in(43.2mm)
Захранване	External 60 Watt 12V@5A Ouput AC Adapter, 90–264 VAC, 50–60 Hz, IEC60320-C14, inlet, FRU	Single 250 watt, 90–264 VAC, 3.5–1.5 A, 50–60 Hz, IEC60320-C14, inlet, вътрешен, фиксиран
Максимална консумация на енергия (вата)	24 вата	85 вата
Максимално излъчване на топлина (BTU/h)	82 BTU/h	290 BTU/h
MTBF (h)	193,772 h	108,944 h
Тегло само на устройството / на доставения пакет lb. (kg)	3.75 lb (1.7 kg) / 6.5 lb (2.95 kg)	16.2 lb (7.3 kg) / 28.2 lb (12.79 kg)
Безопасност в съответствие на нормативната уредба	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Сертификати за сигурност	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1

ЕТ "L&S - St. Mahaldjiiska" • ЕТ "ЛиС - Ст. Махалджийска" • Sofia София L&S

пецификации. (продъжение)

NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115200 bps, No Parity, 8 bits, 1 Stop Bit
2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2x IOTB HDD 3.5", SAS3, 7.2krpm FRU RAID1
1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
17.2in(437mm) x 25.6in(650mm) x 1.7in(43.2mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in (88.4mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in(88.4mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in(88.4mm)	17.2in(437mm) x 31.0in (787mm) x 3.5in(89 mm)
Redundant (1+1) 750 watt, 100–240 VAC, 9–4.5A, 50–60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100–240 VAC, 9–4.5A, 50–60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100–240 VAC, 9–4.5A, 50–60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100–240 VAC, 10.5–4.0A, 50–60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 1000 watt, 100–240 VAC, 10.5–4.0A, 50–60 Hz IEC60320-C14 inlet, FRU
265 вата	426 вата	519 вата	658 вата	660 вата
904 BTU/h	1,454 BTU/h	1,771 BTU/h	2,245 BTU/h	2,252 BTU/h
54,200 h	65,466 h	57,766 h	52;802 h	54,041 h
29.8 lbs (13.5 kg) / 40.8 lbs (18.5 Kg)	37.4 lbs (17.0 kg) / 58.6 lbs (26.6 kg	42.4 lbs (19.2 kg) / 63.5 lbs (28.8 kg)	42.7 lbs (19.2 kg) / 63.8 lbs (29.0 kg)	44 lbs (20 kgs) 71 lbs (32.2Kg)
IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950- UL 60950 CSA/CAN-
FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 L CC NDPP v

Таблица 3. FireEye Network Security smart node, физически спецификации. (продължение)

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
ЕМС съответствие на нормативната уредба	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	Safety: EN 60950; C22.2; UL 60950; IEC 60950; CAN/CSA-C22.2; K 60950; AS/NZS 60950; GB 4943.1; J60950, SI60950 EMC: FCC Part 15 SubPart B Class A; ICES-003; EN55032; VCCI V-3; EN 55024; EN 61000; CNS 13438; CISPR32; KN 32; KN 35
Съответствие с изискванията за опазване на околната среда	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS; REACH; WEEE Conflict Minerals
Работна температура	0–40°C 32–104°F	0–40°C 32–104°F	0–40° C 32–104° F	0–40° C 32–104° F	0–40° C 32–104° F	0–40° C 32–104° F	0–40° C 32–104° F
Температура в изключен режим	-20–80°C -4–176°F	-20–80°C -4–176°F	-30–70° C (-22–158° F)	-40–70°C -40–158°F	-40–70°C -40–158°F	-40–70°C -40–158°F	-30–70°C -22–158°F
Работна относителна влажност	10–95% at 40° C без кондензация	5–85% at 40° C без кондензация	10–95% @ 40° C, без кондензация	10–95% @ 40° C, без кондензация	10–95% @ 40° C, без кондензация	10–95% @ 40° C, без кондензация	10%–90%@40°C - без кондензация
Относителна влажност в изключен режим	10–95% at 60° C без кондензация	5–95% at 40° C без кондензация	10–95% @ 60° C, без кондензация	10–95% @ 60° C, без кондензация	10–95% @ 60° C без кондензация	10–95% @ 60° C без кондензация	10%–95%@55°C без кондензация
Работна височина	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft

Таблица 4. FireEye Network Security smart node IPS, физически спецификации.

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Максимална работа на IPS	До 50 Mbps	До 100 /250 Mbps	До 500 Mbps	До 1 Gbps	До 2 Gbps	До 5 Gbps	До 10 Gbps
Максимални едновремен ни връзки	15K	80K	160K	500K	1M	2M	4M
Нови свързвания за секунда	750/sec	4K/Sec	8K/Sec	10K/Sec	20K/sec	40K/Sec	80K/Sec

Таблица 5. FireEye Network Security smart node, виртуални спецификации.

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
Поддържани операционни системи	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Производителност *	До 50 Mbps	До 100 Mbps	До 250 Mbps	До 500 Mbps	До 1 Gbps
Мрежови портове за мониторинг	1–8	1–8	1–8	1–8	1–8
Портове за управление на мрежата	1 или 2	1 или 2	1 или 2	1 или 2	1 или 2
Режим на работа на мрежовите портове	Inline, SPAN	Inline, SPAN	Inline, SPAN	Inline, SPAN	Inline, SPAN
CPU ядра	3	6	8	8	16
Памет	10GB	16GB	16GB	32 GB	32 GB
Капацитет на диска	384 GB	384 GB	384 GB	512 GB	512 GB
Мрежови адаптери	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC
Поддръжка на хипервизор	VMWare ESXi6.0 or later and KVM 1.5.3 или по-късна версия	VMWare ESXi6.0 or later and KVM 1.5.3 или по-късна версия	VMWare ESXi6.0 or later and KVM 1.5.3 или по-късна версия	VMWare ESXi6.0 or later and KVM 1.5.3 или по-късна версия	VMWare ESXi6.0 or later and KVM 1.5.3 или по-късна версия
Сертификати за сигурност	FIPS 140-2 Level 1 CC NDPP v1.1 (В процес на получаване)	FIPS 140-2 Level 1 CC NDPP v1.1 (В процес на получаване)	FIPS 140-2 Level 1 CC NDPP v1.1 (В процес на получаване)	FIPS 140-2 Level 1 CC NDPP v1.1 (В процес на получаване)	FIPS 140-2 Level 1 CC NDPP v1.1 (В процес на получаване)

Таблица 6. FireEye Network Security smart node IPS, виртуални спецификации.

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
Максимална работа на IPS	До 50 Mbps	До 100 Mbps	До 250 Mbps	До 500 Mbps	До 1 Gbps
Максимални едновременни връзки	15K	80K	80K	160K	500K
Нови свързвания за секунда	750/Sec	4K/Sec	4K/Sec	8K/Sec	10K/Sec

Таблица 7. AMI размери, поддържани от FireEye Network Security на AWS.

Модел	Скорост	vCPU	Памет	Диск	Мрежови интерфейси	Тип AWS Instance
NX4500v	500Mbps	8	32GB	512GB (EBS)	Един порт за управление, един порт за подаване и два порта за мониторинг (общо 4 порта)	M5.2xlarge
NX6500v	1Gbps	16	64GB	512GB (EBS)	Един порт за управление, един порт за подаване и 6 порта за мониторинг (общо 8 порта)	M5.4xlarge

Таблица 8. Спецификации на интелигентната мрежа FireEye MVX.

	VX 5500	VX 12550
Поддържани операционни системи	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Производителност *	До 2 Gbps	До 14 Gbps
Висока наличност **	N+1	N+1
Портове за управление (заден панел)	1x 10/100/1000 Mbps BASE- T	1x 10/100/1000 Mbps BASE- T
Клъстерни портове (заден панел)	3x 10/100/1000 Mbps BASE-T	1x 10/100/1000 Mbps BASE-T, 2x 10 Gbps BASE-T, 4x 10GigE SFP+ портове
IPMI порт (заден панел)	Включен	Включен
Преден LCD и клавиатура	Не са налични	Няма LCD
VGA портове	Включени	Включени
USB портове (заден панел)	4x Type A USB портове	2x Type A USB портове
Сериен порт (заден панел)	115,200 bps, No Parity, 8 bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Капацитет на диска	2x 2TB 3.5" SAS3 HDD, RAID 1, hot-swappable, FRU	2x 4TB 3.5" SAS3 HDD, RAID 1, hot-swappable, FRU
Кутия	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Размер на шасито ШхДхВ	17. 2 x 25.6 x 1.7 in (437 x 650 x 43.2 mm)	17.2 x 31 x 3.5 in (437 x 787 x 89 mm)
DC захранване	Не е налично	Не е налично
AC захранване	Redundant (1+1) 750 watt, 100–240 VAC, 8 - 3.8 A, 50–60 Hz, IEC60320-C14, inlet, hot-swappable, FRU	Redundant (1+1) 1000 watt, 100–240 VAC 10.5–4.0A, 50–60 Hz IEC60320-C14 inlet, FRU
Максимална консумация на енергия (вата)	285 вата	660 вата
Максимално излъчване на топлина (BTU/h)	972 BTU/h	2594 BTU/h
MTBF (h)	54,200 h	54,041 h
Тегло само на устройството / на доставения пакет lb. (kg)	27.0 lbs (12.2 kg) / 38.0 lbs (17.2 kg)	44 lbs (20 kg) / 71 lbs (32.2 kg)
Сертификати за сигурност	FIPS 140-2 Level 1, CC NDPP v1.1 (Предстоящ)	FIPS 140-2 Level 1, CC NDPP v1.1 (Предстоящ)
Безопасност в съответствие на нормативната уредба	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

Таблица 9. Спецификации на интелигентната мрежа FireEye MVX. (продължение)

	VX 5500	VX 12500
ЕМС съответствие на нормативната уредба	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015
Съответствие с изискванията за опазване на околната среда	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU
Работна температура	0–40° C (32–104° F)	0–40°C (32–104°F)
Температура в изключен режим	-30–70° C (-22–158° F)	-30–70°C (-22–158°F)
Работна относителна влажност	10–95% at 40° C без кондензация	10%–90% at 40°C без кондензация
Относителна влажност в изключен режим	10–95% at 60° C без кондензация	10%–95% at 55°C без кондензация
Работна височина	3000 m 9842 ft	3000 m 9842 ft

Услуги за поддръжка

FireEye предлага прости и гъвкави програми за поддръжка, за да увеличи максимално стойността на вашите FireEye продукти и услуги. На разположение са четири различни нива на услуги за поддръжка: Platinum, Platinum Priority Plus, Government и Government Priority Plus. За повече информация относно поддръжката на FireEye, вижте услугите за поддръжка на FireEye.

За да научите повече за FireEye, посетете: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

© 2019 FireEye, Inc. Всички права запазени. FireEye е регистрирана търговска марка на FireEye, Inc. Всички други марки, продукти или услуги са или могат да бъдат търговски марки или марки на услуги на съответните им собственици.
NS-EXT-DS-US-EN-000048-11

За FireEye, Inc.

FireEye е компания за интелигентна охрана. Работейки като безпроблемно, мащабируемо разширение на защитните операции на клиентите, FireEye предлага единна платформа, която съчетава иновативни технологии за сигурност, информация заплахи на национално ниво и световнопризната консултация Mandiant®. С този подход FireEye елиминира сложността и тежестта на киберсигурността за организации, които се борят да се подготвят, предотвратяват и реагират на

Подписаната, Антония Миланова Василева, ЕГН: 8105278498, Потвърждение №: 18ПР-1398/26.02.2018 г., удостоверявам верността на превода от английски на български език на приложения документ –, извършен от мен. Преводът се състои от 12 страници.

Подпис: Антония Миланова Василева

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

FIREEYE™

DATA SHEET

FireEye Network Security

Effective protection against cyber breaches for midsize to large organizations

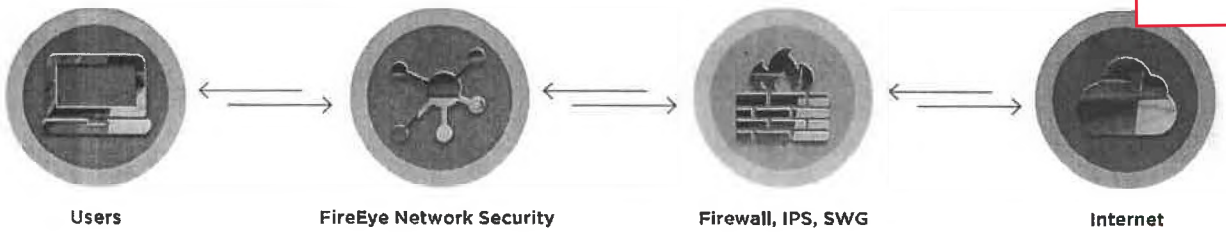
Overview

FireEye Network Security is an effective cyber threat protection solution that helps organizations minimize the risk of costly breaches by accurately detecting and immediately stopping advanced, targeted and other evasive attacks hiding in Internet traffic. It facilitates efficient resolution of detected security incidents in minutes with concrete e, actionable intelligence and response w integration. With FireEye Network , organizations are effectively protected today's threats whether they exploit ft Windows, Apple OS X operating systems, cation vulnerabilities; are directed at the arters or branch offices; or are hidden in a large volume of inbound Internet traffic that has to be inspected in real time.

At the core of FireEye Network Security are the Multi-Vector Virtual Execution™ (MVX) and Intelligence-Driven Analysis (IDA) technologies. MVX is a signature-less, dynamic analysis engine that inspects suspicious network traffic to identify attacks that evade traditional signature- and policy-based defenses. IDA is a collection of contextual, dynamic rules engines that detects and blocks malicious activity in real-time and retroactively, based on the latest machine-, attacker- and victim-intelligence. FireEye Network Security also includes intrusion prevention system (IPS) technology to detect common attacks using conventional signature matching.

FireEye Network Security is available in a variety o form factors, deployment and performance option It is typically placed in the path of Internet traffic behind traditional network security appliances such as next-generation firewalls, IPS and secure web gateways (SWG). FireEye Network Security supplements these solutions by rapidly detecting both known and unknown attacks with high accuracy and a low rate of false positives, while facilitati efficient response to each alert.

Figure 1. Typical configuration — Network Security solutions.



ВЯРНО С ОРИГИНАЛА

Capabilities	Benefits
Detection	
Accurate detection of advanced, targeted and other evasive cyber attacks	Minimizes risk of costly cyber breaches
Extensible, modular security architecture	Provides investment protection
Consistent level of protection for multi-OS environments and all Internet access points	Creates a strong defense across the entire organization for all types of devices
Integrated, distributed, physical, virtual, on-premise and cloud deployment options	Offers flexibility to align with organizational preferences and resources
Multi-vector correlation with Email and Content Security	Provides visibility across wider attack surface
Prevention	
Immediate blocking of attacks at line rates from 10 Mbps to 8 Gbps	Gives real-time protection against evasive attacks
Response	
Low rate of false alerts, riskware categorization and automated IPS alert validation	Reduces operational cost of triaging unreliable alerts
Pivot to investigation and alert validation, endpoint containment and incident response	Automates and simplifies security workflows
Execution evidence and actionable threat intelligence with contextual insight	Accelerates prioritization and resolution of detected security incidents
Scalability from one site to thousands of sites	Supports business growth

ВЯРНО С ОРИГИНАЛА

Technical Advantages

Accurate Threat Detection

FireEye Network Security uses multiple analysis techniques to detect attacks with high accuracy and a low rate of false alerts:

- **Multi-Vector Virtual Execution™ (MVX)** engine detects zero-day, multi-flow and other evasive attacks with dynamic, signature-less analysis in a safe, virtual environment. It stops infection and compromise phases of the cyber-attack kill chain by identifying never-before-seen exploits and malware.
- **Intelligence-Driven Analysis (IDA)** engines detect and block obfuscated, targeted and other customized attacks with contextual, rule-based analysis from real-time insights gathered on the front lines from millions of MVX verdicts, thousands of hours of incident response experience gathered by Mandiant, a FireEye company and hundreds of iSight threat researchers. It stops infection, compromise and intrusion phases of the cyber-attack kill chain by identifying malicious exploits, malware and command and control (CnC) callbacks. It also extracts and submits suspicious network traffic to the MVX engine for a definitive verdict analysis.
- **Structured Threat Intelligence eXpression (STIX)** allows the ingestion of third-party threat intelligence using an industry-standard format to add custom threat indicators into the IDA engines.

Immediate and Resilient Protection

FireEye Network Security offers flexible configuration modes including:

- Out-of-band monitoring via a TAP/SPAN, inline monitoring or inline active blocking. Inline blocking mode automatically blocks inbound exploits and malware and outbound multi-protocol callbacks. In inline monitoring mode, alerts are generated and organizations decide how to respond to them. In out-of-band prevention mode, FireEye Network Security issues TCP resets for out-of-band blocking of TCP, UDP or HTTP connections.
- Selected models offer an active high availability (HA) option to provide resilience in case of network or device failures.

Wide Attack Surface Coverage

FireEye Network Security delivers a consistent level of protection for today's diverse network environments:

- Support for most common Microsoft Windows and Apple Mac OS X operating systems
- Analysis of over 140 different file types, including portable executables (PEs), web content, archives, images, Java, Microsoft and Adobe applications and multimedia
- Execution of suspicious network traffic against thousands of operating system, service pack, application type and applicatio version combinations
- Protection against advanced attacks and malware types that are difficult to detect via signatures: web shell uploads, web shell execution, ransomware, cryptominers

Validated and Prioritized Alerts

In addition to detecting genuine attacks, FireEye MVX technology is also used to determine the reliability of alerts detected by conventional signature-matchin methods and to identify and prioritize critical t

- Intrusion prevention system (IPS) with MV engine validation reduces the time require to triage signature-based detection that i traditionally prone to false alerts
- Riskware categorization separates genuine breach attempts from undesirable, but less malicious activity (such as adware and spyware) to prioritize alert response

Actionable Threat Insights

Alerts generated by FireEye Network Security include concrete evidence and contextual intelligence to quickly respond to, prioritize and contain a threat:

- **Dynamic Threat Intelligence (DTI):** concrete, real-time, globally-shared data to quickly and proactively stop targeted and newly discovered attacks
- **Advanced Threat Intelligence (ATI):** contextual insights about the attack to accelerate response and prescriptive guidance to contain the threat

Response Workflow Integration

FireEye Network Security can be augmented in several ways to automate alert response workflows:

- FireEye Central Management correlates alerts from both FireEye Network Security and FireEye Email Security for a broader view of an attack and to set blocking rules that prevent the attack from spreading further
- FireEye Network Forensics integrates with FireEye Network Security to provide detailed packet captures associated with an alert and enable in-depth investigations
- FireEye Endpoint Security identifies, validates and contains compromises detected by FireEye Network Security to simplify containment and remediation of affected endpoints

Flexible Deployment Options

FireEye Network Security offers various deployment options to match an organization's needs and budget:

- **Integrated Network Security:** standalone, all-in-one hardware appliance with integrated MVX service to secure an Internet access point at a single site. FireEye Network Security is an easy-to-manage, clientless platform that deploys in under 60 minutes. It doesn't require rules, policies or tuning.
- **Distributed Network Security:** extensible appliances with centrally shared MVX service to secure Internet access points within organizations
  - **Network Smart Node:** physical or virtual appliances that analyze Internet traffic to detect and block malicious traffic and submit suspicious activity over an encrypted connection to the MVX service for definitive verdict analysis
  - **MVX Smart Grid:** on-premise, centrally located, elastic MVX service that offers transparent scalability, built-in N+1 fault tolerance and automated load balancing
  - **FireEye Cloud MVX:** FireEye-hosted MVX service subscription that ensures privacy by analyzing traffic on the Network Smart Node. Only suspicious objects are sent over an encrypted connection to the MVX service, where objects revealed as benign are discarded.
  - **Protection on-premise or in the cloud:** In addition to stand-alone and virtual appliances, FireEye offers Network Security in the Public Cloud with the availability of Amazon Machine Images (AMIs).

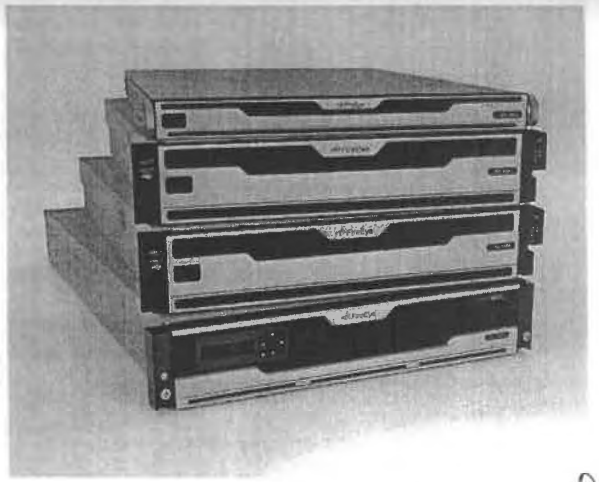


Figure 2. Examples of Integrated Network Security include NX 2550, NX 3500, NX 5500, NX 10550.

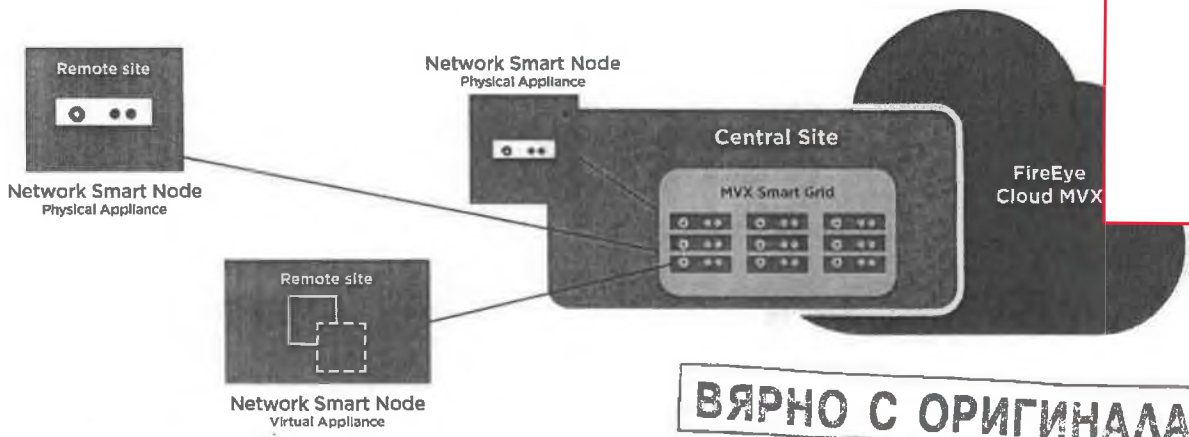


Figure 3. Distributed deployment models for Network Security.

ВЯРНО С ОРИГИНАЛА

Figure 4. Modular components of FireEye Network Security.

High Performance and Scalability

FireEye Network Security protects Internet access points at line rate with performance options for a wide variety of branch and central office sizes:

The MVX Smart Grid and FireEye Cloud MVX scalable architecture allows the MVX service to support one Network Smart Node to thousands and scale seamlessly as needed.

Form Factor	Performance
Integrated Network Security	50 Mbps to 5 Gbps
Physical Network Smart Node	50 Mbps to 10 Gbps
Virtual and Public Cloud Network Smart Node	50 Mbps to 1 Gbps

Business Benefits

Designed to meet the needs of single-site and distributed multi-site organizations, FireEye Network Security delivers several benefits:

Minimizes Risk of Cyber Breaches

FireEye Network Security is a highly-effective cyber defense solution that:

- Prevents intruders from breaking into an organization to steal valuable assets or disrupt business by stopping advanced, targeted and other evasive attacks
- Stops attacks and contains intrusions faster with concrete evidence, actionable intelligence, inline blocking and response workflow automation
- Eliminates weak points from an organization's cyber defenses with consistent protection for various operating systems, application types, branches and central sites

Short Payback Period

According to a recent Forrester Consulting study[1], FireEye Network Security customers can expect a 152% ROI savings over three years and payback on their initial investment in just 9.7 months. FireEye Network Security:

- Focuses security team resources on real attacks to reduce operational expenses
- Optimizes capital spend with a shared MVX service and a large variety of performance points to rightsize deployment to meet requirements
- Future-proofs security investment by scaling smoothly when the number of branches or the amount of Internet traffic grows
- Protects existing investments by allowing cost-free migration from an integrated to a distributed deployment
- Reduces future capital outlay with modular and extensible architecture

Awards and Certifications

The FireEye Network Security product portfolio has been awarded a number of industry and government awards and certifications:

- In 2018, Frost & Sullivan recognized FireEye as the undisputed market leader with 46% market share, more than the next ten competitors combined[2]
- FireEye Network Security has been a recipient of numerous awards from SANS Institut Magazine, CRN and others
- FireEye Network Security was the first security solution on the market to rece US Department of Homeland Security Act Certification

1 Forrester (May 2016). The Total Economic Impact of FireEye.
2 Frost & Sullivan (2018) Advanced Malware Sandbox (AMS) Solutions Market, Global, Forecast to 2022.

ВЯРНО С ОРИГИНАЛА

Table 1. FireEye Network Security specifications, integrated appliance.

	NX 2500	NX 2550
OS Support	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Performance *	Up to 50 Mbps or 100 Mbps	Up to 250 Mbps
Network Monitoring Ports	4x 1GigE Bypass	4x 10GigE SFP+ 4x 1GigE Bypass
Network Ports Mode of Operation	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN
High Availability (HA)	Not Available	Not Available
Management Ports (rear panel)	2x 10/100/1000 BASE- T Ports	2x 1GigE
IPMI Port	Front panel	Rear panel
Front LCD & Keypad	Not Available	Not Available
VGA Port	No	Yes
USB Ports	2x Type A USB Ports (front panel)	4x Type A USB Ports (all rear)
Serial Port (rear panel)	115,200 bps, No Parity, 8 bits, 1 Stop Bit (RJ45 connector RJ45-to-Dsub adapter cable is included)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Drive Capacity	Single 1TB 3.5 inch, SATA HDD, internal, fixed	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1
Enclosure	1RU, Fits 19 inch Rack	1RU, Fits 19-inch Rack
Chassis Dimension WxDxH	17.2in(437mm) x 19.7in(500mm) x 1.7in(43.2 mm)	17.2in(437mm) x 25.6in(650mm) x 1.7in(43.2mm)
AC Power Supply	Single 250 watt, 90-264 VAC, 3.5-1.5 A, 50-60 Hz, IEC60320-C14, inlet, Internal, Fixed	Redundant (1+1) 750 watt, 100-240 VAC 8.0-4.5A, 50-60 Hz IEC60320-C14 inlet, FRU

NX 3500	NX 4500	NX 5500	NX 6500
Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Up to 500 Mbps	Up to 1 Gbps	Up to 2.5 Gbps	Up to 5 Gbps
4x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 2x 40GigE QSFP+
In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line, Monitor,TAP/SPAN
Not Available	Available	Available	Available
2x 1GigE	2x 1GigE	2x 1GigE	2x 1GigE
Rear panel	Rear panel	Rear panel	Rear panel
Not Available	Not Available	Not Available	Not Available
Yes	Yes	Yes	Yes
4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	2x Type A USB Ports
115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115200 bps, No Parity, 8 bits, 1 Stop Bit
2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2x 10TB HDD 3.5", SAS3, 7.2krpm FRU RAID1
2RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack	2RU, Fits 19 inch Rack
17.24in(438mm) x 24.41in(620mm) x 3.48in (88.4mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in(88.4mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in(88.4mm)	17.2in(437mm) x 31.0in(787mm) x 3.5in(89mm)
Redundant (1+1) 800 watt, 100-240 VAC 10.5-4.0A, 50-60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100-240 VAC 10.5-4.0A, 50-60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100-240 VAC 10.5-4.0A, 50-60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 1000 wa 100-240 VAC 10.5-4.0A, 50-60 Hz IEC60320-C14 inlet, FRU

ВЯРНО С ОРИГИНАЛА

Table 1. FireEye Network Security specifications, integrated appliance. (continued)

	NX 2500	NX 2550	NX 3500
Power Consumption Maximum (watts)	85 watts	265 watts	426 watts
Thermal Dissipation Maximum (BTU/h)	290 BTU/h	904 BTU/h	1,454 BTU/hr
MTBF (h)	108,944 h	54,200 h	65,466 h
Appliance Alone / As Shipped Weight lb. (kg)	16.2 lb (7.3 kg) / 28.2 lb (12.79 kg)	29.8 lbs (13.5 Kg) / 40.8 lbs (18.5 Kg)	37.4 lbs (17.0 Kg) / 58.6 lbs (26.6 kg)
Regulatory Compliance Safety	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Security Certifications	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1
Regulatory Compliance EMC	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015
Environmental Compliance	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU
Operating Temperature	0–40°C 32–104°F	0–40°C 32–104°F	0–40°C 32–104°F
Non-Operating Temperature	-20–80°C -4–176°F	-30–70°C -22–158°F	-40–70°C -40–158°F
Operating Relative Humidity	5–85% at 40°C non-condensing	10–95% @ 40° C, non-condensing	10–95% @ 40° C, non-condensing
Non-Operating Relative Humidity	5–85% at 40°C non-condensing	10–95% @ 60° C, non-condensing	10–95% @ 60° C, non-condensing
Operating Altitude	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft

NX 4500	NX 5500	NX 6500
519 watts	658 watts	660 watts
1,771 BTU/h	2,245 BTU/h	2,252 BTU/h
57,766 h	52,802 h	54,041 h
42.4 lbs (19.2 Kg) / 63.5 lbs (28.8 kg)	42.7 lbs (19.2 Kg) / 63.8 lbs (29.0 kg)	44 lbs (20 kgs) 71 lbs (32.2Kg)
IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP vw1.1
FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	Safety: EN 60950; C22.2; UL 60950; IEC 60950; CAN/CSA-C22.2; K 60950; AS/NZS 60950; GB 4943.1; J60950, SI60950 EMC: FCC Part 15 SubPart B Class A; ICES-00[redacted] EN55032; VCCI V-[redacted] 55024; EN 61000; [redacted] 13438; CISPR32; K[redacted] KN 35
RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS; REACH; W[redacted] Conflict Minerals
0-40°C 32-104°F	0-40°C 32-104°F	0-40°C 32-104°F
-40-70°C -40-158°F	-40-70°C -40-158°F	-30-70°C -22-158°F
10-95% @ 40° C, non-condensing	10-95% @ 40° C, non-condensing	10%-90%@40°C non-condensing
10-95% @ 60° C, non-condensing	10-95% @ 60° C, non-condensing	10%-95%@55°C non-condensating
3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft

[redacted]

ВЯРНО С ОРИГИНАЛА

Table 2. FireEye Network Security IPS performance, integrated appliance.

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Max IPS Performance	Up to 50 Mbps or 100 Mbps	Up to 250 Mbps	Up to 500 Mbps	Up to 1 Gbps	Up to 2.5 Gbps	Up to 5 Gbps
Max Concurrent Connections	15K or 80K	80K	160K	500K	1M	2M
New Connections Per Second	750/Sec or 4K/Sec	4K/Sec	8K/Sec	10K/Sec	20K/Sec	40K/Sec

Table 3. FireEye Network Security smart node, physical specifications.

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
OS Support	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Performance	Up to 50 Mbps	Up to 100 Mbps or 250 Mbps	Up to 500 Mbps	Up to 1 Gbps	Up to 2 Gbps	Up to 5 Gbps	Up to 10Gbps
Network Monitoring Ports	4x 10/100/1000 BASE-T Ports	4x 1GigE Bypass	4x 10GigE SFP+ 4x 1GigE Bypass	4x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 2x 40GigE QSFP+
Network Ports Mode of Operation	In-line Monitor, Fail-Close or Tap	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line, Monitor,TAP/ SPAN
High Availability (HA)	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available
Management Ports (rear panel)	2x 10/100/1000 BASE- T Ports	2x 1GigE	2x 1GigE	2x 1GigE	2x 1GigE	2x 1GigE	2x 1GigE
IPMI Port	Not Available	Front panel	Rear panel	Rear panel	Rear panel	Rear panel	Rear panel
Front LCD & Keypad	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available
VGA Port	Not Available	Not Available	Yes	Yes	Yes	Yes	Yes
USB Ports	2x Type A USB Ports	2x Type A USB Ports (front panel)	4x Type A USB Ports (all rear)	4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	2x Type A USB P

ВЯРНО С ОРИГИНАЛА

Table 2: FortiEye Network Security smart node, physical specifications. (continued)

	NX 1500	NX 2500	NX 2550
Serial Port (rear panel)	115,200 bps, No Parity, 8 bits, 1 Stop Bit (RJ45 connector; RJ45-to-Dsub adapter cable is included)	115,200 bps, No Parity, 8 bits, 1 Stop Bit (RJ45 connector RJ45-to-Dsub adapter cable is included)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Drive Capacity	Single 500GB 2.5 inch SATA HDD, internal, fixed	Single 1TB 3.5 inch SATA HDD, internal, fixed	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1
Enclosure	Desktop formfactor	1RU, Fits 19 inch Rack	1RU, Fits 19 inch Rack
Chassis Dimension WxDxH	11in(280mm) x 6.9in(175mm) x 1.7in (44mm)	17.2in(437mm) x 19.7in(500mm) x 1.7in(43.2mm)	17.2in(437mm) x 25.6in(650mm) x 1.7in(43.2mm)
AC Power Supply	External 60 Watt 12V@5A Ouput AC Adapter, 90-264 VAC, 50-60 Hz, IEC60320-C14, inlet, FRU	Single 250 watt, 90-264 VAC, 3.5-1.5 A, 50-60 Hz, IEC60320-C14, inlet, Internal, Fixed	Redundant (1+1) 750 watt, 100-240 VAC, 9-4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU
Power Consumption Maximum (watts)	24 watts	85 watts	265 watts
Thermal Dissipation Maximum (BTU/h)	82 BTU/h	290 BTU/h	904 BTU/h
MTBF (h)	193,772 h	108,944 h	54,200 h
Appliance Alone / As Shipped Weight lb. (kg)	3.75 lb (1.7 kg) / 6.5 lb (2.95 kg)	16.2 lb (7.3 kg) / 28.2 lb (12.79 kg)	29.8 lbs (13.5 kg) / 40.8 lbs (18.5 Kg)
Regulatory Compliance Safety	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Security Certifications	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1

NX 3500	NX 4500	NX 5500	NX 6500
115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115200 bps, No Parity, 8 bits, 1 Stop Bit
2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2x 10TB HDD 3.5", SAS3, 7.2krpm FRU RAID1
2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
17.24in(438mm) x 24.41in(620mm) x 3.48in (88.4mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in(88.4mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in(88.4mm)	17.2in(437mm) x 31.0in (787mm) x 3.5in(89 mm)
Redundant (1+1) 800 watt, 100-240 VAC, 9-4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100-240 VAC, 9-4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100-240 VAC, 10.5-4.0A, 50-60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 1000 watt, 100-240 VAC, 10.5-4.0A, 50-60 Hz IEC60320-C14 inlet, FRU
426 watts	519 watts	658 watts	660 watts
1,454 BTU/h	1,771 BTU/h	2,245 BTU/h	2,252 BTU/h
65,466 h	57,766 h	52,802 h	54,041 h
37.4 lbs (17.0 kg) / 58.6 lbs (26.6 kg	42.4 lbs (19.2 kg) / 63.5 lbs (28.8 kg)	42.7 lbs (19.2 kg) / 63.8 lbs (29.0 kg)	44 lbs (20 kgs) 71 lbs (32.2Kg)
IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level CC NDPP v1.1

ВЯРНО С ОРИГИНАЛА

Table 3. FireEye Network Security smart node, physical specifications. (continued)

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Regulatory Compliance EMC	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	Safety: EN 60950; C22.2; UL 60950; IEC 60950; CAN/CSA-C22.2; K 60950; AS/NZS 60950; GB 4943.1; J60950, SI60950 EMC: FCC Part 15 SubPart B Class A; ICES-003; EN55032; VCCI V-3; EN 55024; EN 61000; CNS 13438; CISPR32; KN 32; KN 35
Environmental Compliance	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS; REACH; WEEE Conflict Minerals
Operating Temperature	0-40°C 32-104°F	0-40°C 32-104°F	0-40° C 32-104° F	0-40° C 32-104° F	0-40° C 32-104° F	0-40° C 32-104° F	0-40° C 32-104° F
Non-Operating Temperature	-20-80°C -4-176°F	-20-80°C -4-176°F	-30-70° C (-22-158° F)	-40-70°C -40-158°F	-40-70°C -40-158°F	-40-70°C -40-158°F	-30-70°C -22-158°F
Operating Relative Humidity	10-95% at 40° C non-condensing	5-85% at 40° C non-condensing	10-95% @ 40° C, non-condensing	10-95% @ 40° C, non-condensing	10-95% @ 40° C, non-condensing	10-95% @ 40° C, non-condensing	10%-90%@40°C non-condensing
Non-Operating Relative Humidity	10-95% at 60° C non-condensing	5-95% at 40° C non-condensing	10-95% @ 60° C, non-condensing	10-95% @ 60° C, non-condensing	10-95% @ 60° C non-condensing	10-95% @ 60° C non-condensing	10%-95%@55°C non-condensating
Operating Altitude	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft

Table 4. FireEye Network Security smart node IPS, physical specifications.

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Max IPS Performance	Up to 50 Mbps	Up to 100 /250 Mbps	Up to 500 Mbps	Up to 1 Gbps	Up to 2 Gbps	Up to 5 Gbps	Up to 10 Gbps
Max Concurrent Connections	15K	80K	160K	500K	1M	2M	4M
New Connections Per Second	750/sec	4K/Sec	8K/Sec	10K/Sec	20K/sec	40K/Sec	80K/Sec

ВЯРНО С ОРИГИНАЛА

Table 5. FireEye Network Security smart node, virtual specifications.

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
OS Support	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Performance *	Up to 50 Mbps	Up to 100 Mbps	Up to 250 Mbps	Up to 500 Mbps	Up to 1 Gbps
Network Monitoring Ports	1-8	1-8	1-8	1-8	1-8
Network Management Ports	1 or 2	1 or 2	1 or 2	1 or 2	1 or 2
Network Ports Mode of Operation	Inline, SPAN	Inline, SPAN	Inline, SPAN	Inline, SPAN	Inline, SPAN
CPU Cores	3	6	8	8	16
Memory	10GB	16GB	16GB	32 GB	32 GB
Drive Capacity	384 GB	384 GB	384 GB	512 GB	512 GB
Network Adapters	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC
Hypervisor Support	VMWare ESXi6.0 or later and KVM 1.5.3 or later	VMWare ESXi6.0 or later and KVM 1.5.3 or later	VMWare ESXi6.0 or later and KVM 1.5.3 or later	VMWare ESXi6.0 or later and KVM 1.5.3 or later	VMWare ESXi6.0 or later and KVM 1.5.3 or later
Security Certifications	FIPS 140-2 Level 1 CC NDPP v1.1 (In Process)	FIPS 140-2 Level 1 CC NDPP v1.1 (In Process)	FIPS 140-2 Level 1 CC NDPP v1.1 (In Process)	FIPS 140-2 Level 1 CC NDPP v1.1 (In Process)	FIPS 140-2 Level 1 CC NDPP v1.1 (In Process)

Table 6. FireEye Network Security smart node IPS, virtual specifications.

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
Max IPS Performance	Up to 50 Mbps	Up to 100 Mbps	Up to 250 Mbps	Up to 500 Mbps	Up to 1 Gbps
Max Concurrent Connections	15K	80K	80K	160K	500K
New Connections Per Second	750/Sec	4K/Sec	4K/Sec	8K/Sec	10K/Sec

Table 7. AMI sizes supported by FireEye Network Security on AWS.

Model	Throughput	vCPU	Memory	Disk	Network Interfaces	AWS Instance Type
NX4500v	500Mbps	8	32GB	512GB (EBS)	One management, one submission and two monitoring ports (total 4 ports)	M5.2xlarge
NX6500v	1Gbps	16	64GB	512GB (EBS)	One management, one submission and six monitoring ports (total 8 ports)	M5.4xlarge

ВЯРНО С ОРИГИНАЛА

Table 8. FireEye MVX smart grid specifications.

	VX 5500	VX 12550
OS Support	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Performance *	Up to 2 Gbps	Up to 14 Gbps
High Availability **	N+1	N+1
Management Ports (rear panel)	1x 10/100/1000 Mbps BASE- T	1x 10/100/1000 Mbps BASE- T
Cluster Ports (rear panel)	3x 10/100/1000 Mbps BASE-T	1x 10/100/1000 Mbps BASE-T, 2x 10 Gbps BASE-T, 4x 10GigE SFP+ ports
IPMI Port (rear panel)	Included	Included
Front LCD & Keypad	Not Available	No LCD
VGA Ports	Included	Included
USB Ports (rear panel)	4x Type A USB Ports	2x Type A USB Ports
Serial Port (rear panel)	115,200 bps, No Parity, 8 bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Drive Capacity	2x 2TB 3.5" SAS3 HDD, RAID 1, hot-swappable, FRU	2x 4TB 3.5" SAS3 HDD, RAID 1, hot-swappable, FRU
Enclosure	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Chassis Dimension WxDxH	17. 2 x 25.6 x 1.7 in (437 x 650 x 43.2 mm)	17.2 x 31 x 3.5 in (437 x 787 x 89 mm)
DC Power Supply	Not Available	Not Available
AC Power Supply	Redundant (1+1) 750 watt, 100–240 VAC, 8 - 3.8 A, 50–60 Hz, IEC60320-C14, inlet, hot-swappable, FRU	Redundant (1+1) 1000 watt, 100–240 VAC 10.5–4.0A, 50–60 Hz IEC60320-C14 inlet, FRU
Power Consumption Maximum (watts)	285 watts	660 watts
Thermal Dissipation Maximum (BTU/h)	972 BTU/h	2594 BTU/h
MTBF (h)	54,200 h	54,041 h
Appliance Alone / As Shipped Weight lb. (kg)	27.0 lbs (12.2 kg) / 38.0 lbs (17.2 kg)	44 lbs (20 kg) / 71 lbs (32.2 kg)
Security Certification	FIPS 140-2 Level 1, CC NDPP v1.1 (Pending)	FIPS 140-2 Level 1, CC NDPP v1.1 (Pending)
Regulatory Compliance Safety	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

ВЯРНО С ОРИГИНАЛА

	VX 5500	VX 12500
Regulatory Compliance EMC	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015
Environmental Compliance	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU
Operating Temperature	0–40° C (32–104° F)	0–40°C (32–104°F)
Non-Operating Temperature	-30–70° C (-22–158° F)	-30–70°C (-22–158°F)
Operating Relative Humidity	10–95% at 40° C non-condensing	10%–90% at 40°C non-condensing
Non-Operating Relative Humidity	10–95% at 60° C non-condensing	10%–95% at 55°C non-condensing
Operating Altitude	3000 m 9842 ft	3000 m 9842 ft

Support Services

FireEye offers simple and flexible support programs to maximize the value of your FireEye products and services. Four different levels of support services are available: Platinum, Platinum Priority Plus, Government and Government Priority Plus. For more information about FireEye support, refer to FireEye Support services.

ВЯРНО С ОРИГИНАЛА

To learn more about FireEye, visit: **www.FireEye.com**

Fi
60 lvd. Milpitas, CA 95035
877.FIREEYE (347.3393)
inf om

© 2 nc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners.
NS-EXT-DS-US-EN-000048-1

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™

Stiliyana Mahaldjiiska
L&S TRANSLATION OFFICE

Превод от английски език!

FIREEYE

Строго поверително

06.07.2020 г.

До:
Информационно обслужване АД
Ул. „Панайот Волов“ 2
1527 София, България

Относно:
Открита процедура „Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите'' с Уникален номер на поръчката 05948-2020-0004, Обособена позиция № 6: „Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити кибер заплахи“.

Уважаеми господа,

Ние, FireEye Ireland Limited (наричано по-нататък „FireEye“), с адрес: 2 Парк Плейс, Сити Гейт Парк, Махон, Корк, Ирландия, с настоящото упълномощаваме нашия дистрибутор „КОМПЮТЪР 2000 България“ ЕООД, с адрес: бул. „Шипченски проход“ 63, София 1574, България, (наричано по-долу „Участник в търга“), да предложи решения на FireEye, на които FireEye е единственият производител, за препродажба или участие в търга по проекта с Уникален номер на поръчката № 05948-2020-0004 в Република България.

С настоящото разширяваме упълномощаването на Участника в търга да извършва гаранционното обслужване на оборудването / системите и да предостави поддръжка Ниво 1. Участникът в търга ще предостави нашата пълна гаранция за предлаганите и доставени от него продукти съобразно с нашите Крайноклиентски условия, налични на: https://www.fireeye.com/company/legal.html и нашата Политика за край на жизнения цикъл на продуктите е налична на: https://www.fireeye.com/support/programs.html.

Моля, не се колебайте да се свържете с нас за допълнителна информация

С уважение,
Подпис: не се чете
Емет Ръсел, Директор
FireEye Ireland Limited

L&S - St. Mahaldjiiska" Sofia L&S София "ЛиС - Ст. Махалджийска"

0002548

ЕТ „Л и С - Стилияна Махалджийска“
Офис „Изток“: 1113 София, ул. Жолио Кюри 46Б, тел./факс: 02 963 44 04
Офис „Младост 1“: 1784 София, бул. Йерусалим, бл. 54, офис 11, партер (в двора), тел./факс: 02 974 57 55
Офис „Бизнес парк София“: 1715 София, Бизнес парк София, сграда 8, вх. А - Б, тел.: 02 489 81 55
ЕТ „L&S - Stiliyana Mahaldjiiska“
Office „Istok“: 1113 Sofia Bulgaria, 46B, Fr. J. Curie Str., tel./fax: 02 963 44 04
Office „Mladost 1“: 1784 Sofia Bulgaria, 54, Yerusalim Blvd., Office 11, ground floor, tel./fax: 02 974 57 55
Office „Business Park Sofia“: 1715 Sofia Bulgaria, Business Park Sofia, building 8, ent. A-B, tel.: +359 2 489 81 55
office@variante.info
sliai@abv.bg
+359 888 875 932
www.variante.info

FireEye Ireland Limited | 2 Парк Плейс, Сити Гейт Парк, Махон, Корк, Ирландия | Регистриран в Ирландия под регистрационен номер на компанията 523830 | Директори: S. Gethin, E. Russell, R. Kelleher | info@FireEye.com | www.FireEye.com | +353 21 6019100

© 2017 FireEye, Inc. Всички права запазени. FireEye е регистрирана търговска марка на FireEye, Inc. Всички други имена на марки, продукти или услуги са или могат да бъдат търговски марки или марки на услуги на съответните им собственици. LH. EN-US.062017

Аз, долуподписаната, Вилислава Стефанова Атанасова, удостоверявам верността на превода от английски на български език на приложения документ, извършен от мен. Преводът се състои от 2 страница.
Подпис: Вилислава Стефанова Атанасова

[redacted]

[redacted]

[redacted]

[redacted]

.velope ID: 11D2CA9A-0291-4A25-BB07-8CC664F83420

FIREEYE

Strictly Confidential

To: Information Services JSC
2 Panayot Volov Str.
1527 Sofia Bulgaria

7/6/2020

Reference: Open Procedure "Delivery of communication equipment, hardware and software, required for the update of the information and communication systems of the National Revenue Agency" with Ref № 05948-2020-0004, LOT 6 "Delivery of hardware appliances and software packages for a protection platform against existing and newly discovered cyber threats".

Dear Sirs,

We, FireEye Ireland Limited (hereinafter "FireEye"), having an address of 2 Park Place, City Gate Park, Mahon, Cork, Ireland, do hereby authorize our distributor COMPUTER 2000 Bulgaria Ltd., 63 Shipchenski prohod Blvd., Sofia 1574, Bulgaria (hereinafter "the Bidder") to offer FireEye solutions of which FireEye is the sole manufacturer, for resale or bid on the project with ref. № 05948-2020-0004 in the Republic of Bulgaria.

We hereby extend their authorization for the Bidder to perform the warranty service of the equipment/systems and to provide Support Level 1. The Bidder will provide our full guarantee and warranty for the products offered and supplied by them in accordance with our End User Terms available at https://www.fireeye.com/company/legal.html and our End of Life Policy available at https://www.fireeye.com/support/programs.html.

Please do not hesitate to contact us for any additional information.

Yours faithfully,

[redacted]

Emmet Russell, Director
FireEye Ireland Limited

ВЯРНО С ОРИГИНАЛА

[redacted]

© 2017 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. LH. EN-US.062017

[redacted]

[redacted]

Stiliyana Mahaldjiska
L&S TRANSLATION OFFICE

Продуктова брошура

FireEye Endpoint Security

Спрете атаките с натрупани познания от защита от първа линия

АКЦЕНТИ

- Предотвратява по-голямата част от кибер атаките срещу крайните точки на средата
- Открива и блокира случващи се нарушения, за да намали въздействието на нарушението
- Подобрява производителността и ефективността чрез разкриване на заплахи, а не преследване на сигнали
- Използва единичен агент с малък отпечатък за минимално въздействие на крайния потребител
- Защити и функционалност чрез модули, които може да бъдат изтегляни
- Отговаря на разпоредби като PCI-DSS и HIPAA
- Внедряване на място или в облака

Сигурността на традиционните крайни точки не е ефективна срещу съвременните заплахи; никога не е била проектирана, за да се справи със сложни заплахи или напреднали постоянни атаки (APT). За да запазите крайните точки в безопасност, решението трябва бързо да види заплахата и да реагира с най-ефективната технология.

FireEye Endpoint Security съчетава най-доброто от наследените продукти за сигурност, подобрено с технологията, експертизата и информацията на FireEye за защита срещу днешните кибер атаки. Въз основа на модел за защита в дълбочина, Endpoint Security използва модулна архитектура със софтуери по подразбиране и модули за сваляне, за да защитава, открива и реагира и управлява агенти.

За да предотврати разпространението на вирусен софтуер, Endpoint Security използва софтуер за защита на крайната точка (EPP), базиран на дефиниции. За да намери заплахи, за които все още няма дефиниция, MalwareGuard използва машинно обучение, богато с натрупана информация от първата линия на борбата с кибер атаките. За да се справят с напредналите заплахи, възможностите за откриване и реакция на крайни точки (EDR) се активират чрез механизъм за анализ на основата на поведението. Решението работи на базата на индикатори за компроментиране (IOC), които се анализират в реално време, като се разчита на текущата информация от първа линия, за да се спомогне за намирането на скрити заплахи. За да добавите нови софтуери и функции, можете да изтеглите модули от FireEye Market.

Дори при най-добрата защита нарушенията са неизбежни. За да осигури ефективна реакция, която минимизира смущенията в бизнес процесите, Endpoint Security предоставя инструменти за:

- Търсене и проучване на известни и неизвестни заплахи за десетки хиляди крайни точки за минути
- Идентифициране и изготвяне на подробни вектори на атака, използвана за проникване в крайна точка
- Определяне дали атака е възникнала (и продължава) към конкретна крайна точка и къде се е разпространила
- Предоставяне на времедиаграма и продължителност на даден инцидент, довел до компроментиране на крайни точки и проследяване на инцидента
- Ясно определяне на това кои крайни точки и системи се нуждаят от ограничаване, за да се предотвратят последващи зловредни действия

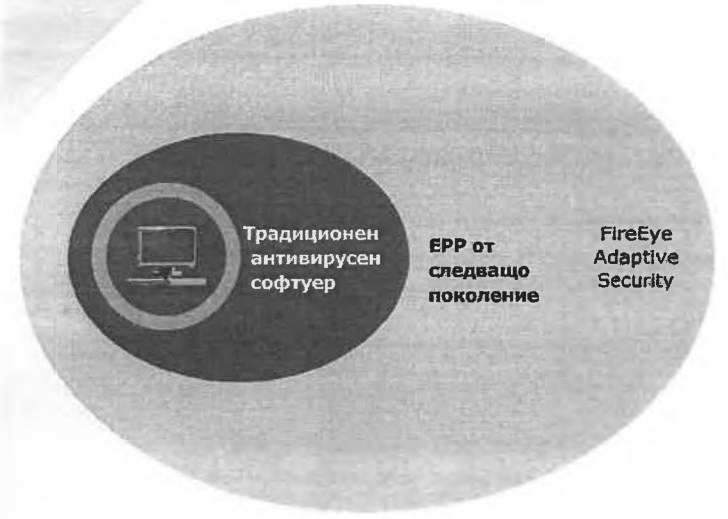
ИТ са стратегически фактор, който движи способността ни за ефективно обучение на нашите студенти. Използването на FireEye Endpoint Security гарантира, че нашите ИТ активи са достъпни, високо функциониращи и сигурни, което е изключително важно за постигането на нашата мисия.

— James D. Perry II
Главен експерт информационна сигурност, Университет на Северна Каролина

0002459

ЕТ „Я[redacted]лияна Махалджийска"
Офис „Изток": 1113 София, ул. Жолио Кюри 46Б, тел./факс: 02 963 44 04
Офис „Младост 1": 1784 София, бул. Йерусалим, бл. 54, офис 11, партер, [redacted] 974 57 55
Офис „Бизнес парк София": 1715 София, Бизнес парк София, сграда 8, вх. А - Б, тел.: [redacted] 89 81 55
ЕТ „L&S - Stiliyana Mahaldjiska"
Office „Istok": 1113 Sofia Bulgaria, 46B, Fr. J. Curie Str., tel./fax: 02 963 44 04
Office „Mladost 1": 1784 Sofia Bulgaria, 54, Yerusalim Blvd., Office 11, ground floor, [redacted]
Office „Business Park Sofia": 1715 Sofia Bulgaria, Business Park Sofia, building 8, [redacted]55

office@variante.info
sliai@abv.bg
+359 888 875 932
www.variante.info



Често ръководството смята, че всеки вирус е почти краят на света. С FireEye мога да предложа истински доказателства за същността на проблема и за това, че сме успели да го управляваме и спрем. Превръщането на всички тези неизвестни в ясна информация бързо помага да се намали натиска за всички в организацията.

— **Michael Hennessy,** Директор Технологични услуги
Alpha Grainer Manufacturing, Inc

Поддържани операционни системи и среди	
Windows	Windows 7, 8, 8.1, 10 Server 2008R2, 2012R2, 2016, 2019
Mac	OS X 10.9+
Linux	RedHat Enterprise Linux 6.8+, 7.2+, 8 CentOS 6.8+, 7.2+, 8 Ubuntu 14.04, 16.04, 18.04 SUSE 11.3, 11.4, 12.2, 12.3, 15 Open SUSE 15.1 Amazon AMI 2018.3, AMI2 Oracle Linux 6.10 & 7.6

Опции за внедряване: физически уред на място, виртуален уред на място, облачна услуга FireEye

Основни функции

- Единичен агент, използващ защита в дълбочина, за да се сведе до минимум конфигурацията и да се увеличи максимално откриването и блокирането
- Единичен интегриран работен поток за анализ и реагиране на заплахи в Endpoint Security
- Напълно интегрирана защита от вирусен софтуер използвайки антивирусни (AV) защити, машинно обучение, анализ на поведението, индикатори за компрометиране (IOC) и видимост на крайната точка
- Обобщение на прегледа и одитна проверка за изчерпателна проверка и анализ на заплахите

Допълнителни функции

- Enterprise Security Search за бързо намиране и показване на подозрителна активност и заплахи
- Придобиване на данни за извършване на подробна интензивна инспекция и анализ на крайните точки при определен времеви график
- Видимост от край до край, която позволява на екипите за сигурност бързо да търсят, идентифицират и различават нивото на заплахите
- Възможности за откриване и отговор за бързо намиране, проучване и спиране на крайни точки за ускоряване на реакцията
- Лесен за разбиране интерфейс за бърза интерпретация и реакция на всяка подозрителна крайна точка

AV.TEST MITRE VirusTotal

За да научите повече за FireEye, посетете: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2020 FireEye, Inc. Всички права запазени. FireEye е регистрирана търговска марка на FireEye, Inc. Всички други марки, продукти или услуги са или могат да бъдат търговски марки или марки на услуги на съответните им собственици. EP-EXT-DS-US-EN-000018-05

За FireEye, Inc.

FireEye е компания за интелигентна охрана. Работейки като безпроблемно, мащабируемо разширение на защитните операции на клиентите, FireEye предлага единна платформа, която съчетава иновативни технологии за сигурност, информация заплахи на национално ниво и световнопризната консултация Mandiant®. С този подход FireEye елиминира сложността и тежестта на киберсигурността за организации, които се борят да се подготвят, предотвратяват и реагират на кибератаки..

FIREEYE™

ЕТ "ЛиС - Ст. Махалджийска" * ЕТ "Lab - St. Mahaldjiisk..." * Sofia Lab София

Подписаната, Антония Миланова Василева, ЕГН: 8105278498, Потвърждение №: 18ПР-1398/26.02.2018 г., удостоверявам верността на превода от английски на български език на приложения документ –, извършен от мен. Преводът се състои от 3 страници.
Подпис: Антония Миланова Василева

[redacted]

[redacted]

[redacted]

[redacted]

FIREEYE™

DATA SHEET

FireEye Endpoint Security

Stop attacks with knowledge from frontline responses

HIGHLIGHTS

- Prevent the majority of cyber attacks against the endpoints of an environment
- Detect and block breaches that occur to reduce the impact of a breach
- Improve productivity and efficiency by uncovering threats rather than chasing alerts
- Use a single, small-footprint agent for minimal end-user impact
- Protections and functionality through downloadable modules
- Comply with regulations, such as PCI-DSS and HIPAA
- Deploy to onsite or in the cloud

Traditional endpoint security is not effective against modern threats; it was never designed to deal with sophisticated or advanced persistent threat (APT) attacks. To keep endpoints safe, a solution must quickly see the threat and respond with the most effective technology.

FireEye Endpoint Security combines the best of legacy security products, enhanced with FireEye technology, expertise and intelligence to defend against today's cyber attacks. Based on a defense in depth model, Endpoint Security uses a modular architecture with default engines and downloadable modules to protect, detect and respond and manage agents.

To prevent common malware, Endpoint Security uses a signature-based endpoint protection platform (EPP) engine. To find threats for which a signature does not yet exist, MalwareGuard uses machine learning seeded with knowledge from the frontlines of cyber attacks. To deal with advanced threats, endpoint detection and response (EDR) capabilities are enabled through a behavior-based analytics engine. A real-time indicators of compromise (IOC) engine relies on current, frontline intelligence to help find hidden threats. To add new engines and features, you can download modules from the FireEye Market.

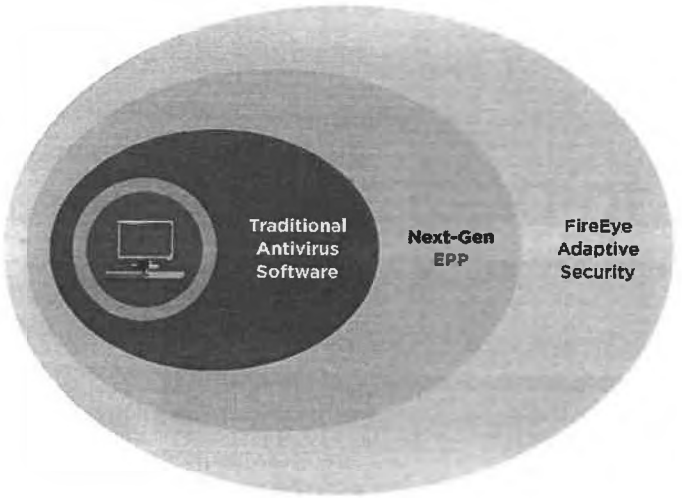
Even with the best protection, breaches are inevitable. To ensure a substantive response that minimizes business disruption, Endpoint Security provides tools to:

- Search for and investigate known and unknown threats on tens of thousands of endpoints in minutes
- Identify and detail vectors an attack used to infiltrate an endpoint
- Determine whether an attack occurred (and persists) on a specific endpoint and where it spread
- Establish timeline and duration of endpoint compromises and follow the incident
- Clearly identify which endpoints and systems need containment to prevent further compromise

IT is a strategic enabler that drives our ability to effectively educate our students. Utilizing FireEye Endpoint Security ensures that our IT assets are available, highly functioning, and secure, which is critical to achieving our mission.

— James D. Perry II
Chief Information Security Officer, University of South Carolina

ВЯРНО С ОРИГИНАЛА



Often, management thinks any virus is almost the end of the world. With FireEye, I can bring real evidence to display about the nature of the issue and that we've been able to manage and contain it. Making all of those unknowns known quickly helps to take the pressure down for everybody in the organization.

— Michael Hennessy, Director Technology Services
Alpha Grainer Manufacturing, Inc

Primary Features

- Single agent using defense in depth to minimize configuration and maximize detection and blocking
- Single integrated workflow to analyze and respond to threats within Endpoint Security
- Fully integrated malware protection with antivirus (AV) defenses, machine learning, behavior analysis, indicators of compromise (IOCs) and endpoint visibility
- Triage Summary and Audit Viewer for exhaustive inspection and analysis of threats

Additional Features

- Enterprise Security Search to rapidly find and illuminate suspicious activity and threats
- Data Acquisition to conduct detailed in-depth endpoint inspection and analysis over a specific time frame
- End-to-end visibility that allows security teams to rapidly search for, identify and discern the level of threats
- Detection and response capabilities to quickly detect, investigate and contain endpoints to expedite response
- Easy-to-understand interface for fast interpretation and response to any suspicious endpoint activity

Supported Operating Systems and Environments	
Windows	Windows 7, 8, 8.1, 10 Server 2008R2, 2012R2, 2016, 2019
Mac	OS X 10.9+
Linux	RedHat Enterprise Linux 6.8+, 7.2+, 8 CentOS 6.8+, 7.2+, 8 Ubuntu 14.04, 16.04, 18.04 SUSE 11.3, 11.4, 12.2, 12.3, 15 Open SUSE 15.1 Amazon AMI 2018.3, AMI2 Oracle Linux 6.10 & 7.6

Deployment options: onsite physical appliance, onsite virtual appliance, FireEye Cloud Service

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2020 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. EP-EXT-DS-US-EN-000018-05

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

ВЯРНО С ОРИГИНАЛА

ПРИЛОЖЕНИЕ №1

към ТЕХНИЧЕСКОТО ПРЕДЛОЖЕНИЕ за ОБОСОБЕНА ПОЗИЦИЯ № 6:

„Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити кибер заплахи“

ОБЩИ УСЛОВИЯ

за гаранционно обслужване от производителя **FIREEYE**

на продуктите, предмет на обществената поръчка **„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите''**,

по Обособена позиция № 6: „Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити кибер заплахи“

Настоящите гаранционни условия се отнасят за дефекти, възникнали в следствие процеса на нормална експлоатация по време на гаранционния период. Гаранционният срок на софтуерните и хардуерните продукти започва да тече от датата на издаване на лицензионния сертификат от производителя и обхваща периода зададен в сертификата.

Производителят **FIREEYE** доставя своите софтуерни и хардуерни продукти със Платинено ниво на поддръжка (**FireEye Platinum Support**). Платиненото ниво на поддръжка осигурява софтуерна и хардуерна поддръжка от типа **24x7x365**. **Времето за реакция** при критични проблеми е **до един бизнес ден.**

Платиненото ниво на поддръжка обхваща закупените софтуерни и хардуерни решения и абонаменти услуги и включва:

- 24x7 достъп до обновления на софтуерните и хардуерните продукти на производителя;
- 24x7 поддръжка, която се предоставя чрез няколко канала за комуникация: чат канал, уеб портал, телефонно обаждане, чрез email съобщения;
- Незабавно ескалиране на инциденти от степен 1 до екип от ниво 3 за инженерна поддръжка на производителя, ако заявката е обсъдена и чрез телефонно обаждане, за да се изяснят изискванията на клиента и необходимите ресурси от FireEye;

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- Документи описващи най-актуалните препоръки за ефективно ползване на продуктите на производителя и други препоръчани стъпки за отстраняване на нежелани проблеми, както и документация описваща разликите в най-новите версии на софтуерните и хардуерните решения на производителя;
- Достъп до специално разработени „кръпки“ от производителя, тествани и с потвърдено качество от инженерния екип на FireEye, за подадени заявки за техническа поддръжка за инциденти от степен1;
- Възможност за отстраняване на повреди и несъответствия на предоставеното от производителя хардуерно оборудване, съответно възможност за подмяна на дефектирало хардуерно устройство с ново, в рамките на предоставените гаранционни условия от производителя за закупените решения;
- Достъп до защитен портал на производителя за техническа поддръжка FireEye Support Portal, който съдържа:
    - Портал за подаване и проследяване на заявки за техническа поддръжка към производителя за закупените решения;
    - Достъп до форум общност на производителя за търсене на информация и водене на дискусия с потребители на FireEye от целият свят;
    - Достъп до онлайн база от данни с документация на производителя, която съдържа ръководства за имплементация и експлоатация на решенията им, както и документация за известни проблеми и стъпки за отстраняване им;
    - Информация за нови версии/обновления на продуктите на производителя
    - Други известия

Времената за реакция на техническия екип на производителя при подаване на информация за технически неизправности, при Платинена поддръжка с достъпност тип 24x7x365, са както следва:

- За инциденти от степен 4 – минорни инциденти, които не водят до прекъсване на процеси и услуги на софтуерните продукти – отговор до 8 часа;
- За инциденти от степен 3 – средни или минорни инциденти, които водят до кратко прекъсване или неизправност на процеси и услуги на софтуерните продукти – отговор до 4 часа;
- За инциденти от степен 2 – големи инциденти, които водят до сериозно ограничаване или прекъсване на процеси и услуги на софтуерните продукти, но не спиращи изцяло работния процес на организацията – отговор до 2 часа;

[redacted]

[redacted]

- За инциденти от степен 1 – критични инциденти, които водят до трайно прекъсване на процеси и услуги на софтуерните продукти и спиране на работния процес на организацията – отговор до 30 минути;

Повече информация има на следния адрес: https://www.fireeye.com/support/programs.html

Дата на подписване:	13/ 07 / 2020
Подпис и печат:	.....
Име и фамилия	Анелия Костадинова
Длъжност	Управител
Наименование на участника	„КОМПЮТЪР 2000 България“ ЕООД

ПРИЛОЖЕНИЕ №2

към ТЕХНИЧЕСКОТО ПРЕДЛОЖЕНИЕ за ОБОСОБЕНА ПОЗИЦИЯ № 6:

„Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити кибер заплахи“

ОБЩИ УСЛОВИЯ

за извършване на доставки и гаранционна поддръжка

от фирма КОМПЮТЪР 2000 България ЕООД

Настоящите условия за доставки и гаранционна поддръжка се отнасят за дефекти, възникнали в следствие процеса на нормална експлоатация по време на гаранционния период и не ограничава по никакъв начин действащите закони и други задължителни разпоредби в Република България. Гаранционният срок на хардуерните устройства и софтуерните продукти е в съответствие със закупеното ниво на техническа поддръжка и започва да тече от датата на приемо-предавателния протокол за доставка.

Доставяните от КОМПЮТЪР 2000 България хардуерни и софтуерни продукти са винаги фабрично нови, неупотребявани, в актуалните продуктови листи на производителите към датата на доставките и не са спрени от производство. Хардуерните компоненти на оборудването отговарят на всички стандарти в Република България относно ергономичност, пожарна безопасност, норми за безопасност и включване към електрическата мрежа.

Хардуерното оборудване се доставя винаги в пълно работно състояние, в оригиналната опаковка на производителя с ненарушена цялост, окомплектовано с всички необходими интерфейсни и захранващи кабели, в случай, че са различни от стандартни IEC C14 - IEC C13 или IEC C20 - IEC C19. Необходимата техническа документация, като потребителски, инсталационни, конфигурационни и др. ръководства се представят на електронен носител за всеки тип устройства. При доставка на софтуер се предоставят необходимите сертификати и/или други документи, удостоверяващи предоставеното право на ползване на софтуера.

С настоящите Общи условия се гарантира пълната функционална годност на доставеното оборудване/доставения софтуер съгласно предписанията на производителя.

Процедурата по гаранционната поддръжка от страна на КОМПЮТЪР 2000 България ЕООД се базира на стандартите БДС EN ISO 9001:2015, БДС ISO/IEC 27001:2017.

В рамките на гаранционния срок и в съответствие със закупеното ниво на техническа поддръжка се отстраняват за наша сметка всички повреди и/или несъответствия на оборудването, съответно подменят дефектирали части, устройства, модули и/или компоненти с нови съгласно предписанията на производителя. В гаранционното обслужване се включва замяна на част (компонент) със скрити недостатъци с нова или на цялото устройство с ново, ако недостатъкът го прави негодно за използване по предназначението му, както и всички разходи по замяната.

Режимът на гаранционното обслужване на хардуерните продукти е 5 дни в седмицата (от понеделник до петък), 8 часа в рамките на работното време от 9.00 ч. до 17.30 ч. Подаването на сервизна заявка към КОМПЮТЪР 2000 България може да бъде извършено следните e-mail или телефон:

- Телефон: 02 439 2000, 02 439 2009
- e-mail адрес: software@computer2000.bg

Времето за реакция е до следващия работен ден от уведомяването от клиента. „Време за реакция“ е времето от момента на уведомяване от страна на клиента за възникнал проблем до обратна реакция (обаждане или пристигане на място) от наша страна. Осигуряваме и преглед на място в срок не по-късно от следващия работен ден от 9.00 ч. до 17.30 ч.

Настъпилата повреда и/или несъответствие се отстранява до възстановяване на пълната работоспособност на оборудването. Отстраняването на настъпила повреда и/или несъответствието се осъществява по местоположение на оборудването. При невъзможност за отстраняване на настъпила повреда и/или несъответствие в срок от следващите два работни дни, се осигурява оборотно оборудване, сходно по технически характеристики с доставеното на клиента, включително доставка на нови алтернативни решения при запазване на пълната изисквана функционалност, до пълното отстраняване на повреда или несъответствие, като срокът на гаранционно обслужване на оборудването в процеса на поправяне, се удължава със срока, през който е траело отстраняването на повредата.

В случай, че повредата и/или несъответствието прави устройството негодно за използване по предназначението му, ние го заменяме с ново, с параметри, гарантиращи същата или по-добра функционалност и производителност.

За всяка извършена дейност, свързана с гаранционната поддръжка, се изготвя и предоставя протокол, който съдържа описание на извършеното. Протоколът се подписва от представители на двете страни. На всяко тримесечие се предоставя обобщен отчет за извършените дейности по гаранционно обслужване, които се приемат от клиента. В обобщените отчети се посочва най-малко следната информация: период на покритие на отчета и списък с възникналите проблеми и

параметрите, при които са отстранени проблемите. Всички разходи по време на гаранционното обслужване са за наша сметка.

Дата на подписване:	10/ 07 / 2020
Подпис и печат:	.....
Име и фамилия	Анелия Костадинова
Длъжност	Управител
Наименование на участника	„КОМПЮТЪР 2000 България“ ЕООД

ПРИЛОЖЕНИЕ № 3.6

ДО
„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД
ГР. СОФИЯ, УЛИЦА „ПАНАЙОТ ВОЛОВ“ № 2

ЦЕНОВО ПРЕДЛОЖЕНИЕ

Наименование на обществената поръчка:	***„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите“***
Наименование на обособена позиция, за която участникът подава оферта	***Обособена позиция № 6: „Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити киберзаплахи“***
Наименование на участника:	***КОМПЮТЪР 2000 България***
Правно-организационна форма на участника:	***ЕООД***
Седалище по регистрация и адрес на управление:	**Бул. „Шипченски проход“ № 63, ет. 4, Производствена сграда „Електроника“, гр. София 1574**
ЕИК / Код по регистър БУЛСТАТ/ регистрационен номер или друг идентификационен код:	**831816173**
Представляващ	***Анелия Илиева Костадинова - Управител***

Заличаването на информация в документа е на основание чл. 4 от Общ регламент за защита на данните.

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,

След запознаване с документацията за участие в обществената поръчка с горепосочения предмет, ние предоставяме следното ценово предложение по горецитираната обособена позиция:

1. Предлагаме да изпълним доставката, предмет на горецитираната процедура за възлагане на обществена поръчка при следните цени:

№	Описание	Количество	Единична цена в лв. без ДДС	Обща цена в лв. без ДДС
I.	II.	III.	IV.	V.
1.	Подсистема за засичане, разследвания и защита от познати и непознати заплахи на ниво крайна точка	1 брой	871 392.00	871 392.00
2.	Подсистема за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения	1 брой	1 059 042.00	1 059 042.00
3.	Подсистема за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво	1 брой	1 366 776.00	1 366 776.00
4.	Подсистема за централизирано управление	1 брой	88 792.00	88 792.00
5.	Подсистема за централизирано разтоварване на процесите по извършване на динамичен анализ на зловреден код и на кибератаки от другите подсистеми за киберсигурност	1 брой	1 189 620.00	1 189 620.00
6.	Подсистема (лаборатория) за динамичен анализ на зловреден код	1 брой	165 940.00	165 940.00
7.	Подсистема за динамичен анализ на зловреден код и защита от кибератаки за мрежови файлови дялове (лаборатория) за динамичен анализ на зловреден код	1 брой	254 595.00	254 595.00
8.	Подсистема за улавяне на мрежови пакети, разследвания и централизиран анализ и визуализация	1 брой	384 348.00	384 348.00
			Обща цена в лева без ДДС	5 380 505.00

2. В цените по т. 1 са включени всички разходи за изпълнение на поръчката. Потвърждаваме, че възложителят няма да дължи заплащането на каквито и да е други разноски, направени от нас като изпълнител.

3. Потвърждаваме, че цените по т. 1 са постоянни за целия срок на договора и не подлежат на промяна за времето на изпълнение на договора, освен в случаите когато това е в полза на възложителя.

Приложения: ***Приложение №1 - Количествено-стойностна сметка към Ценовото***

предложение

Забележка:

1. *Предложените от участника цени следва да са в български лева без ДДС, закръглени до втория знак на десетичната запетая.*

2. *Участник, който допусне аритметична грешка, се отстранява от участие в процедурата по съответната обособена позиция.*

3. *Участник, който предложи обща цена, която е по-висока от прогнозната стойност на съответната обособена позиция, се отстранява от по-нататъшно участие в процедурата по съответната обособена позиция.*

4. *Липсата на ценово предложение, както и предоставянето на ценово предложение, което не отговаря на изискванията на документацията за обществената поръчка, е основание за отстраняване от по-нататъшно участие в процедурата по съответната обособена позиция.*

Дата на подписване:	**10/ 07 / 2020**
Подпис и печат:	**.....**
Име и фамилия	**Анелия Костадинова**
Длъжност	**Управител**
Наименование на участника	**„КОМПЮТЪР 2000 България“ ЕООД**

ПРИЛОЖЕНИЕ №1

към Ценовото предложение

на фирма „КОМПЮТЪР 2000 България“ ЕООД

по *Обособена позиция № 6: „Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити киберзаплахи“*

КОЛИЧЕСТВЕНО-СТОЙНОСТНА СМЕТКА

1. **Подсистема за засичане, разследвания и защита от познати и непознати заплахи на ниво крайна точка**

Продукт	Продуктов №	Бр.	Единична цена в лв. без ДДС	Обща цена в лв. без ДДС
Хардуерно устройство FireEye HW-4502 HX	4502HX-HW	1	26,670.00	26,670.00
Платинена поддръжка на хардуерно устройство FireEye 4502 HX за 5 години	4502HX-PTM-5Y	1	25,235.00	25,235.00
Хардуерно устройство FireEye HW-4502D HX DMZ	4502DHX-HW	1	18,677.00	18,677.00
Платинена поддръжка на хардуерно устройство FireEye HW-4502D HX DMZ за 5 години	4502DHX-PTM-5Y	1	16,810.00	16,810.00
Софтуерни лицензи за поставяне на крайните точки FireEye Endpoint Security Power-9999	90HXSA-9999	8000	28.00	224,000.00
Абонамент за прилежащи услуги към софтуерните лицензи DTI Endpoint Security Power Off Sub-9999 за 5 години	90HXSA-OFDTI-9999-5Y	8000	45.00	360,000.00
Платинена поддръжка на софтуерни лицензи за поставяне на крайните точки FireEye Endpoint Security Power-9999 за 5 год.	90HXSA-PTM-9999-5Y	8000	25.00	200,000.00
			Обща цена в лв. без ДДС	871,392.00

[redacted]

[redacted]

[redacted]

2. **Подсистема за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения**

Продукт	Продуктов №	Бр.	Единична цена в лв. без ДДС	Обща цена в лв. без ДДС
Хардуерно устройство FireEye 8500EX-HW EMAIL MPS	8500EX-HW	2	97,915.00	195,830.00
Платинена поддръжка на хардуерно устройство FireEye 8500EX-HW EMAIL MPS за 5 години	8500EX-PTM-5Y	2	83,378.00	166,756.00
Абонамент за прилежащи услуги към хардуерните устройства FireEye DTI 8500 EX Off sub за 5 години	8500EX-OFDTI-5Y	2	148,228.00	296,456.00
Абонамент за софтуерни лицензи за анализиране на прикачени файлове и URL адреси в email съобщенията FireEye Attach/URL engine-9999 за 5 години	90EX-9999-5Y	8000	50.00	400,000.00
			Обща цена в лв. без ДДС	1,059,042.00

3. **Подсистема за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво**

Продукт	Продуктов №	Бр.	Единична цена в лв. без ДДС	Обща цена в лв. без ДДС
Хардуерно устройство FireEye HW-NX 5500	5500NX-HW	2	199,140.00	398,280.00
Платинена поддръжка на хардуерно устройство FireEye HW NX 5500 за 5 години	5500NX-PTM-5Y	2	174,037.00	348,074.00
Абонамент за прилежащи услуги към хардуерните устройства FireEye DTI NX 5500 Off-5Y за 5 год.	5500NX-OFDTI-5Y	2	309,400.00	618,800.00
Хардуерни разширителни модули 1G-10G BASE-LX/LR FIBER	LXLR1G10G-HW	2	811.00	1,622.00
			Обща цена в лв. без ДДС	1,366,776.00

[redacted]

4. Подсистема за централизирано управление

Продукт	Продуктов №	Бр.	Единична цена в лв. без ДДС	Обща цена в лв. без ДДС
Хардуерно устройство FireEye 7500CM-HW CMS	7500CM-HW	1	47,792.00	47,792.00
Платинена поддръжка на хардуерно устройство FireEye 7500CM-HW CMS за 5 години	7500CM-PTM-5Y	1	41,000.00	41,000.00
			Обща цена в лв. без ДДС	88,792.00

5. Подсистема за централизирано разтоварване на процесите по извършване на динамичен анализ на зловреден код и на кибератаки от другите подсистеми за киберсигурност

Продукт	Продуктов №	Бр.	Единична цена в лв. без ДДС	Обща цена в лв. без ДДС
Хардуерно устройство FireEye HW-MVX Compute 12550	12550VX-HW	2	173,535.00	347,070.00
Платинена поддръжка на хардуерно устройство FireEye HW-MVX Compute 12550 за 5 години	12550VX-PTM-5Y	2	151,659.00	303,318.00
Абонамент за прилежащи услуги към хардуерните устройства FireEye DTI 12550 MVX Compute Off за 5 години	12550VX-OFDTI-5Y	2	269,616.00	539,232.00
			Обща цена в лв. без ДДС	1,189,620.00

[redacted]

6. **Подсистема (лаборатория) за динамичен анализ на зловреден код**

Продукт	Продуктов №	Бр.	Единична цена в лв. без ДДС	Обща цена в лв. без ДДС
Хардуерно устройство FireEye 5550AX-HW MAS	5550AX-HW	1	50,190.00	50,190.00
Платинена поддръжка на хардуерно устройство FireEye 5550AX-HW MAS за 5 години	5550AX-PTM-5Y	1	41,670.00	41,670.00
Абонамент за прилежащи услуги към хардуерното устройство FireEye DTI AX 5550 Off sub за 5 години	5550AX-OFDTI-5Y	1	74,080.00	74,080.00
			Обща цена в лв. без ДДС	165,940.00

7. **Подсистема за динамичен анализ на зловреден код и защита от кибератаки за мрежови файлови дялове (лаборатория) за динамичен анализ на зловреден код**

Продукт	Продуктов №	Бр.	Единична цена в лв. без ДДС	Обща цена в лв. без ДДС
Хардуерно устройство FireEye HW-6500 FX	6500FX-HW	1	75,650.00	75,650.00
Платинена поддръжка на хардуерно устройство FireEye HW-6500 FX за 5 години	6500FX-PTM-5Y	1	64,420.00	64,420.00
Абонамент за прилежащи услуги към хардуерното устройство: FireEye DTI 6500 FX Off за 5 години	6500FX-OFDTI-5Y	1	114,525.00	114,525.00
			Обща цена в лв. без ДДС	254,595.00

8. **Подсистема за улавяне на мрежови пакети, разследвания и централизиран анализ и визуализация**

Продукт	Продуктов №	Бр.	Единична цена в лв. без ДДС	Обща цена в лв. без ДДС
Хардуерно устройство FireEye HW 2060ESS96 PX	2060ESS96-PX-HW	1	108,590.00	108,590.00
Платинена поддръжка на хардуерно устройство FireEye HW 2060ESS96 PX за 5 години	2060ESS96-PX-PTM-5Y	1	90,157.00	90,157.00
Хардуерно устройство с вграден софтуер за централизиран анализ и визуализация FireEye HW 2100HN48 IA	2100HN48-IA-HW	1	102,542.00	102,542.00
Платинена поддръжка на хардуерно устройство FireEye HW 2100HN48 IA за 5 години	2100HN48-IA-PTM-5Y	1	83,059.00	83,059.00
			Обща цена в лв. без ДДС	384,348.00

Дата на подписване:	10/ 07 / 2020
Подпис и печат:	.....
Име и фамилия	Анелия Костадинова
Длъжност	Управител
Наименование на участника	„КОМПЮТЪР 2000 България“ ЕООД