Приложение № 2
към рамков договор № ИС-28/02.10.2023 г.

Заявка

по рамков договор № ИС-28 от 02.10.2023 г.

Позиция от ПГ-2024 г.:	*№ по ред от ПГ*	*17*
Описание на дейност/проект съгласно ПГ:	*Обновяване на информационната и комуникационната инфраструктура на Агенция по геодезия, картография и кадастър*	
CPV код	*32522000 – Телекомуникационно оборудване*	
Изискване за достъп до класифицирана информация ДА/НЕ	*Не*	
Стойност: (*стойността следва да съответства на заложената в План-графика***) без ДДС**		*Обща стойност 2 419 540 лева*
Срок за плащане: *(еднократно, на части, периодично или др.)*		*На части. След подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на съответната доставка.*
Плащане с акредитив ДА/НЕ		*Не*
Документи за плащане с акредитив		*Не*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**		*до 30.06.2024 г*
Гаранционен срок:		*5 години за всеки компонент от Техническите параметри, считано от датата на приемо-предавателния протокол по чл. 6 от договора, удостоверяващ приемане на съответната доставка*
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*		*На части. С подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на съответната доставка*
Приложения: (*напр: технически параметри,образци на отчетни документи*)		*Технически параметри*
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		
ЗАЯВКАТА е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:		
Координатор по заявката:		
Ръководител на проект/дейност по заявката (напр: представител на дирекцията – Заявител):		
Ръководител на договора от страна на ВЪЗЛОЖИТЕЛЯ:		

ЗАЯВКАТА е ОДОБРЕНА ОТ:	
За Главен счетоводител на АГКК:	
Изпълнителен директор на АГКК:	
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:	
Координатор от „Информационно обслужване“ АД по заявката	
Ръководител на проект/дейност по заявката	
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД	

Заличаванията в документите са на основание чл. 4 от Общия регламент относно защитата на данните – Регламент (ЕС) 2016/679.

ТЕХНИЧЕСКИ ПАРАМЕТРИ ЗА

ОБНОВЯВАНЕ НА ИНФОРМАЦИОННАТА И КОМУНИКАЦИОННА ИНФРАСТРУКТУРА НА АГКК

I. Цел на заявката

Целта на настоящата заявка е да осигури обновяване на информационната и комуникационна инфраструктура на АГКК с цел опазване сигурността, надеждността и работоспособността на системите в мрежата на АГКК.

II. Обхват на заявката

Настоящата заявка обхваща доставката на следното оборудване:

1. Комутатор тип 1 – количество 28 броя

Технически изисквания	
REQ.1.	Монтаж - в 19“ шкаф.
REQ.2.	Токозахранване - AC.
REQ.3.	48 порта 1GE RJ45 и 4 порта 1GE SFP модули.
REQ.4.	Брой USB портове – 1.
REQ.5.	Сериен конзолен порт – 1.
REQ.6.	Изолиране на потребителите от един и същ VLAN.
REQ.7.	Идентификация и оторизация на достъпа: 802.1x идентификация и оторизация с прилагането на динамични VLAN и ACL. MAC authentication bypass. Идентификация чрез вграден Web портал. Комбиниране на методите за идентификация на един порт – 802.1x, MAC адрес, WEB идентификация. RADIUS CoA.
REQ.8.	Хардуерно реализирани листи за филтриране на трафика, на база source/destination IP адреси, source/destination MAC адреси, протоколи и Layer 4 TCP/UDP номера на портове.
REQ.9.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимален брой пакети в секунда
REQ.10.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимална скорост в секунда.
REQ.11.	DHCP Snooping или еквивалентен метод.
REQ.12.	DHCP опция 82.
REQ.13.	Dynamic ARP inspection или еквивалентен метод.
REQ.14.	IP source guard или еквивалентен метод за защита от IP spoofing в мрежи с динамично и статично присвояване на IP адресите.
REQ.15.	Автоматично запаметяване на използвания от първото клиентското у-во MAC адрес и блокиране на мрежовия достъп за други устройства, които се свързват към същия порт.
REQ.16.	Spanning Tree защити - BPDU Guard и Root Guard.
REQ.17.	Хардуерно IP forwarding и комутиране със следните параметри: Производителност – 100 Gbps. Forwarding – 75 Mpps. MAC адреси – 16000.

	IPv4 + IPv6 маршрути – минимум 900. Multicast маршрути – 1000.
REQ.18.	DRAM – 512 MB.
REQ.19.	Jumbo frames - 9000 байта.
REQ.20.	Spanning Tree – IEEE 802.1d, 802.1w и 802.1s.
REQ.21.	Функция Private VLAN.
REQ.22.	Разпознаване на мрежова връзка с еднопосочна пропускливост между два комутатора от същия вид.
REQ.23.	Рутинг протоколи: Статично рутиране
REQ.24.	IEEE 802.3ad LACP протокол.
REQ.25.	IEEE 802.1AB (LLDP) и LLDP-MED.
REQ.26.	QoS със следните функции, като минимум: Групиране на трафика в трафични класове на база Layer2, Layer 3 и Layer 4 трафични параметри, 802.1p и DCSP маркировка. Traffic policing. Traffic shaping. Поддръжка на две приоритетни опашки (PQ) на порт. Поддръжка на Weighted Tail Drop (WTD) или еквивалентен алгоритъм за управление на задръствания. Поддръжка на Weighted Random Early Detection (WRED) или еквивалентен алгоритъм за предотвратяване на задръствания. DSCP и 802.1p маркиране на трафика на база трафични политики.
REQ.27.	Протоколи и функции за управление и наблюдение: Web GUI. CLI. DNS. TFTP. FTP. NTP. SSHv2 и SNMPv3. Вграден DHCP сървър. Задаване ниво на достъп до системата за всеки администратор. Идентификация на администраторите чрез външни RADIUS или TACACS+ системи. Управление през Bluetooth.
REQ.28.	Комплект планки за монтаж в 19“ шкаф
REQ.29.	Хардуерна гаранция за срок от минимум 5 (пет) години.
REQ.30.	Техническа поддръжка за срок от минимум 5 (пет) години.
REQ.31.	Получаване на нови версии на софтуера за срок от минимум 5 (пет) години.

2. Защитна стена тип 1 – количество 26 броя

Технически изисквания	
REQ.1.	Минимална пропускателна способност с активирана функция за идентификация на приложенията (appmix) – 1.0 Gbps
REQ.2.	Минимална пропускателна способност с активирани всички функционалности за защита: IPS/ AntiVirus/AntiMalware/URL/ Firewall/ Application Control – 0.5 Gbps

REQ.3.	Минимална производителност за IPsec VPN – 0.8 Gbps
REQ.4.	Минимален брой сесии - 62 000
REQ.5.	Минимален брой нови сесии в секунда - 10 000
REQ.6.	Разпознати и поддържани приложения (минимум) - 4 200 броя
REQ.7.	Минимален брой мрежови интерфейси: ● Да разполага 7 x Base-T ports
REQ.8.	Режими на работа на интерфейсите: ● L2 ● L3 ● Tap ● Transparent ● едновременно/микс да се използват върху едно устройство.
REQ.9.	Машрутизиращи протоколи: ● OSPFv2/v3 ● BGP with graceful restart ● RIP ● Static routing ● Policy-based forwarding ● Point-to-Point Protocol over Ethernet (PPPoE)
REQ.10.	Минимални изисквания към IPSec имплементация: ● Key exchange: manual key, IKEv1 and IKEv2 (pre-shared key, certificate authentication) ● Encryption: 3DES, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
REQ.11.	Минимален брой конкурентни SSL VPN потребителя включени в системата (постоянни лицензи) - 220 SSL VPN потребителя,
REQ.12.	Устройството да поддържа виртуални таблици за маршрутизация
REQ.13.	Всички конфигурации за интерфейсните модули на защитната стена трябва да поддържат IPv6 както и всички контролни функции на системата трябва да се налични и за IPv6
REQ.14.	Системата следва да декриптира и инспектира SSL като поддържа: TLS v1.1, TLS v1.2, TLS v1.3
REQ.15.	Всяко от устройствата в системата да има възможност да се управлява посредством имплементация на REST based API, извличане на данни и репорти в XML формати. Всяко от устройствата в системата следва да поддържа всеки един от следните методи за управление: CLI, уеб конзола, централизирана система за управление
REQ.16.	Режим на надеждност: ● Active-Passive ● Active/Active
REQ.17.	Минимален брой делегирани интерфейси за управление (в допълнение на мрежовите интерфейси): ● 1 x 10/100/1000 out-of-band management port ● 1 x RJ-45 конзолен порт ● 2 x USB port
REQ.18.	Предназначена за вграждане в 19‘‘шкаф с максимален размер 1U
REQ.19.	Резервирано, 100-240VAC (50-60Hz)
REQ.20.	Изграждане на сектори с различна степен на доверие, които да разделят мрежата на отделни сегменти и прилагане на политики на база потребителски имена от Активната Директория;
REQ.21.	Системата да анализира съдържанието за наличие на зловреден код като включва

	минимум AntiVirus, AntiSpyware, IPS;
REQ.22.	Системата да прави анализ на непознати заплахи (Zero Day зловреден код) в защитена среда като създава и дистрибутира сигнатури в реално време;
REQ.23.	Системата за анализ на Zero Day зловреден код трябва да използва минимум следните методи за анализ: Static Analysis, Machine Learning, Dynamic Analysis, Bare metal analysis
REQ.24.	Системата да анализира PE и PowerShell скриптове в защитната стена и предоставя защита в реално време;
REQ.25.	Системата следва да инспектира за заплахи HTTPS протокола чрез декриптиране;
REQ.26.	Системата следва да инспектира за заплахи HTTP 1.1 и HTTP 2.0 протоколи;
REQ.27.	Администратора трябва да може да изисква прекатегоризация на даден URL директно от графични интерфейс на защитната стена.
REQ.28.	Управлението на устройството трябва да се реализира че физически отделени процесор и памет отделени от ресурсите използвани за управление на трафика;
REQ.29.	Решението да използва вътрешните ресурси на защитната стена за да анализира и открива зловреден JavaScript с цел кражба на корпоративни потребителски имена и пароли чрез Phishing;
REQ.30.	Наличие на DLP (Data Loss Prevention) функционалност, за ограничаване на движението на конфиденциални файлове към и извън организацията;
REQ.31.	Решението да притежава възможност да ограничава достъпа на потребителите до Web сървъри, които не поддържа минимални изисквания за валиден публичен сертификат и съответно високо ниво на сигурност (TLSv 1.1, TLSv1.2, TLSv1.3);
REQ.32.	Да може да препраща подозрителните DNS заявки към устройството с цел ограничаване на достъпа и регистриране на заразени машини в мрежата;
REQ.33.	Предложението решение трябва може да изгражда отдалечен VPN достъп чрез агент инсталиран на крайно клиентската машина;
REQ.34.	Агента за VPN достъп трябва да поддържа (да може да бъде инсталиран) минимум следните операционни системи: Windows, macOS
REQ.35.	Възможност за QoS трафика според типа приложение потребител и/или URL категория;
REQ.36.	Прозрачна идентификация на потребителите от Активната директория без изискване на крайната машина да се инсталира агент, настройки в browser или отваряне на Web Portal;
REQ.37.	Решението да може да изпраща декриптирани потоци от данни към трети страни
REQ.38.	Да предоставя възможност за карантина на заразени устройства независимо от техните IP адреси, локация и потребител.
REQ.39.	Да предоставя възможност чрез допълнителен лиценз за съставяне на политика за сигурност базирана на устройство независимо от неговия IP Address, локация и потребител.
REQ.40.	Решението да може да чете данните в X-Forwarded-For (XFF) за идентифициране на реалния източник на данни (IP Address), когато той се намира зад други мрежови устройства.
REQ.41.	Защита на корпоративните потребителски имена и пароли, посредством блокиране или ограничаване на тяхното използване в външни за организацията системи и публично достъпни доставчици (Dropbox, Google, Facebook, LinkedIn).
REQ.42.	Решението да включва функционалност позволяваща служебния достъп до публични облачни услуги като Office 365, Google, Dropbox и YouTube, и ограничаваща достъпа до лични потребителски акаунти за същите приложения.
REQ.43.	Решението да притежава Уеб базиран интерфейс и да бъде интегрирано, управлявано от предложената облачна система за управление
REQ.44.	Гененираните отчети и логове следва да са обогатени с данни за потребител и група, получена от интеграция с бази за управление на потребителите (Active Directory, LDAP и други);
REQ.45.	Решението да може автоматично да тегли IP, Domain или URL листи от Web Server

	собственост възложителя или външна организация с цел ограничаване / позволяване на достъпа до гореспоменатите.
REQ.46.	Решението да може автоматично да открива какви приложения работят в организацията и да предлага лист от такива, които да бъдат добавени към нови или вече съществуващи правила за сигурност.
REQ.47.	Решението да предоставя механизъм за откриване и превенция на DNS Tunneling канали за комуникация, включително да следи и ограничаване достъпа до автоматично генерирани домейни (Domain generation algorithms (DGA));
REQ.48.	Решението да има SD WAN функционалност за управление на трафика като предлага минимум следните възможности • Събиране на метрики на връзката, джитър, загуби, закъснение • Интелигентен избор на пътя, базиран на метрика • Динамично насочване на приложението • Мащабируеми двупосочни измервания на състоянието на пътя, качество на обслужване, оформяне на трафика • Откриване на дублиране на пакетите
REQ.49.	Системата да има възможност за надграждане с допълнителен лиценз инсталиран на защитната стена, чрез който да осъществява отдалечен защитен достъп от устройства (телефони таблети, персонални компютри) с операционни системи Linux, iOS, Raspbian, Ubuntu, Android. Да извършва инспекция (compliance check) на крайно клиентската машина, който се извършва по време на изграждането на защитена връзка;
REQ.50.	Системата да има възможност за надграждане с допълнителен лиценз инсталиран на защитната стена, с който да открива и управлява IoT (Internet of Things) устройства като предоставя възможност за автоматично генериране на препоръчани правила за достъп и контрол.
REQ.51.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя.
REQ.52.	Хардуерна гаранция за срок от минимум 5 (пет) години.
REQ.53.	Техническа поддръжка за срок от минимум 5 (пет) години.
REQ.54.	Получаване на нови версии на софтуера за срок от минимум 5 (пет) години.

3. Система за централизирано управление на защитните стени съвместима с предложените защитни стени тип 1 – количество 1 брой

Технически изисквания	
REQ.1	Предложената централизирана система за управление следва да е съвместима и позволява управлението на защитните стени
REQ.2	Предложената централизирана система за управление на защитни стени следва да позволява събиране, съхранение и анализ на логове
REQ.3	Предложената централизирана система за управление на защитни стени следва да позволява налагането на политики за сигурност чрез предварително дефинирани профили
REQ.4	Предложената централизирана система за управление на защитни стени следва да позволява централизирана конфигурация на защитните стени като: интерфейси маршрутизиращи протоколи и SDWAN
REQ.5	Предложената централизирана система за управление на защитни стени следва да позволява групиране на устройствата и създаване на йерархична структура
REQ.6	Предложената централизирана система за управление на защитни стени следва да позволява централизирано внедряване на актуализации и нови версии

REQ.7	Автоматизирано внедряване на политики за динамични среди
REQ.8	Предлага базирани на XML и JSON REST API за лесна интеграция
REQ.9	Системата трябва да разполага с предварително дефинирани отчети които да могат да се генерират отделно или по групи
REQ.10	Системата да разполага с доклади за активност на потребителите използваните приложения, посетени URL категории, уебсайтове посетени URL адреси, за определен период от време за отделни потребители.
REQ.11	Предложената централизирана система за управление на защитни стени следва да позволява инсталация върху виртуална машина
REQ.12	Предложената централизирана система за управление на защитни стени следва да поддържа минимум следните среди за виртуализация: • VMWARE ESXi • MS Hyper-V • KVM
REQ.13	Софтуерна гаранционна поддръжка 365x24x7 за минимум 5 (пет) години. Участника следва да използва необходимите лицензи за гаранционна поддръжка от Производителя. Доказва се чрез посочване на партиден номер.

4. Защитна стена тип 2 – количество 2 броя

Технически изисквания	
REQ.1.	Пропускателна способност с активирана функция за идентификация на приложенията - 11.0 Gbps
REQ.2.	Пропускателна способност с активирани всички функционалности за защита: IPS/ AntiVirus/AntiMalware/URL/Firewall/Application Control - 5.1 Gbps
REQ.3.	Производителност за IPsec VPN - 6.8 Gbps
REQ.4.	Брой TCP сесии - 1 400 000
REQ.5.	Брой нови сесии в секунда - 145 000
REQ.6.	Разпознати и поддържани приложения - 4 150 броя
REQ.7.	Брой мрежови интерфейси: • Разполага с 12x 1G/2.5G/5G/10G порта • Разполага с 10x 1G/10G SFP/SFP+ интерфейса • Разполага с 4x 25G SFP28 интерфейса
REQ.8.	Режими на работа на интерфейсите: • L2 • L3 • Tap • Transparent • едновременно/микс да се използват върху едно устройство.
REQ.9.	Машрутизиращи протоколи: • OSPFv2/v3 • BGP with graceful restart • RIP • Static routing • Policy-based forwarding • Point-to-Point Protocol over Ethernet (PPPoE) • Bidirectional Forwarding Detection (BFD)

REQ.10.	Минимални изисквания към IPSec имплементация: • Key exchange: manual key, IKEv1 and IKEv2 (pre-shared key, certificate authentication) • Encryption: 3DES, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
REQ.11.	Минимален брой конкурентни SSL VPN потребителя включени в системата (постоянни лицензи) - 1800 SSL VPN потребителя,
REQ.12.	Минимален брой IPSec Site-to-Site VPN - 5000 отдалечени точки.
REQ.13.	Устройството да поддържа виртуални таблици за маршрутизация минимум 50 броя.
REQ.14.	Устройството да има възможност да поддържа виртуализация (виртуални контексти) – 10 броя.
REQ.15.	Всички конфигурации за интерфейсните модули на защитната стена трябва да поддържат IPv6 както и всички контролни функции на системата трябва да се налични и за IPv6
REQ.16.	Системата следва да декриптира и инспектира SSL като поддържа : TLS v1.1, TLS v1.2, TLS v1.3
REQ.17.	Всяко от устройствата в системата да има възможност да се управлява посредством имплементация на REST based API, извличане на данни и репорти в XML формати. Всяко от устройствата в системата следва да поддържа всеки един от следните методи за управление: CLI, уеб конзола, централизирана система за управление
REQ.18.	Режим на надеждност: • Active-Passive • Active/Active Клъстер до 6 устройства разпределени в отдалечени центрове за данни.
REQ.19.	Минимален брой делегирани интерфейси за управление (в допълнение на мрежовите интерфейси): • 1x 100/1000 out-of-band management port • 2 x 100/1000Mbps, 1 x 10Gbps SFP+ интерфейси за отказоустойчивост • 1 x RJ-45 конзолен порт
REQ.20.	Предназначена за вграждане в 19‘‘ шкаф с максимален размер 1U
REQ.21.	Резервирано, 100-240VAC (50-60Hz)
REQ.22.	Изграждане на сектори с различна степен на доверие, които да разделят мрежата на отделни сегменти и прилагане на политики на база потребителски имена от Активната Директория;
REQ.23.	Системата да анализира съдържанието за наличие на зловреден код като включва минимум AntiVirus, AntiSpyware, IPS;
REQ.24.	Системата да прави анализ на непознати заплахи (Zero Day зловреден код) в защитена среда като създава и дистрибутира сигнатури в реално време;
REQ.25.	Системата за анализ на Zero Day зловреден код трябва да използва минимум следните методи за анализ: Static Analysis, Machine Learning, Dynamic Analysis, Bare metal analysis
REQ.26.	Предлаганата защитна стена трябва да може да изпраща минимум 6000 файла на час към системата за анализ на Zero Day;
REQ.27.	Системата да анализира PE и PowerShell скриптове в защитната стена и предоставя защита в реално време;
REQ.28.	Системата следва да инспектира за заплахи HTTPS протокола чрез декриптиране;
REQ.29.	Системата следва да инспектира за заплахи HTTP 1.1 и HTTP 2.0 протоколи;
REQ.30.	NGFW възможностите и прилежащите бази данни като Antivirus, Sandboxing трябва да използват сигнатури и съдържание на производителя на защитната стена – Не се приема OEM или интеграция с трети страни;
REQ.31.	Управлението на устройството трябва да се реализира че физически отделени процесор и памет отделени от ресурсите използвани за управление на трафика;
REQ.32.	Решението да използва вътрешните ресурси на защитната стена за да анализира и открива

	зловреден JavaScript с цел кражба на корпоративни потребителски имена и пароли чрез Phishing;
REQ.33.	Наличие на DLP (Data Loss Prevention) функционалност, за ограничаване на движението на конфиденциални файлове към и извън организацията;
REQ.34.	Решението да притежава възможност да ограничава достъпа на потребителите до Web сървъри, които не поддържа минимални изисквания за валиден публичен сертификат и съответно високо ниво на сигурност (TLSv 1.1, TLSv1.2, TLSv1.3);
REQ.35.	Препращане на подозрителните DNS заявки към устройството с цел ограничаване на достъпа и регистриране на заразени машини в мрежата;
REQ.36.	Предложението решение трябва може да изгражда отдалечен VPN достъп чрез агент инсталиран на крайно клиентската машина;
REQ.37.	Агента за VPN достъп трябва да поддържа (да може да бъде инсталиран) минимум следните операционни системи: Windows, Linux, macOS, Android, iOS, Raspbian, Ubunto
REQ.38.	Възможност за QoS трафика според типа приложение потребител и/или URL категория;
REQ.39.	Прозрачна идентификация на потребителите от Активната директория без изискване на крайната машина да се инсталира агент, настройки в browser или отваряне на Web Portal;
REQ.40.	Решението да може да изпраща декриптирани потоци от данни към трети страни за допълнителен анализ след което отново да криптира трафика.
REQ.41.	Да предоставя възможност за карантина на заразени устройства независимо от техните IP адреси, локация и потребител.
REQ.42.	Да предоставя възможност за съставяне на политика за сигурност базирана на устройство независимо от неговия IP Address, локация и потребител.
REQ.43.	Решението да може да чете данните в X-Forwarded-For (XFF) за идентифициране на реалния източник на данни (IP Address), когато той се намира зад други мрежови устройства.
REQ.44.	Защита на корпоративните потребителски имена и пароли, посредством блокиране или ограничаване на тяхното използване в външни за организацията системи и публично достъпни доставчици (Dropbox, Google, Facebook, LinkedIn).
REQ.45.	Решението да включва функционалност позволяваща служебния достъп до публични облачни услуги като Office 365, Google, Dropbox и YouTube, и ограничаваща достъпа до лични потребителски акаунти за същите приложения.
REQ.46.	Анализът на логовете и репортинг да се извършва от самото устройство с през неговия графичен интерфейс, без да необходима инсталация на допълнителен софтуер.
REQ.47.	Решението да притежава Уеб базиран интерфейс с различни статистики на база време, приложение, категории, потребители, заплахи и други;
REQ.48.	Гененираните отчети и логове следва да са обогатени с данни за потребител и група, получена от интеграция с бази за управление на потребителите (Active Directory, LDAP и други);
REQ.49.	Решението да може автоматично да тегли IP, Domain или URL листи от Web Server собственост на АГКК или външна организация с цел ограничаване / позволяване на достъпа до гореспоменатите.
REQ.50.	Решението да може автоматично да открива какви приложения работят в организацията и да предлага лист от такива, които да бъдат добавени към нови или вече съществуващи правила за сигурност.
REQ.51.	Решението да предоставя механизъм за откриване и превенция на DNS Tunneling канали за комуникация, включително възможност да следи и ограничаване достъпа до автоматично генерирани домейни (Domain generation algorithms (DGA));
REQ.52.	Системата да има възможност за надграждане с допълнителен лиценз за филтриране на уеб сайтовете по категории и ограничаване на достъпа до опасно съдържание в Интернет, включително мулти категоризация на URL съгласно тип на съдържанието и риск. Да има възможност да анализира URL и тяхното съдържание в реално време. Всяка заявка за

	достъп да бъде анализирана чрез Machine Learning на база на HTTP Request, включително да може да идентифицира новорегистрирани домейни и ограничава достъпа до тях;
REQ.53.	Системата да има възможност за надграждане с допълнителен лиценз инсталиран на защитната стена, чрез който да осъществява отдалечен защитен достъп от телефони и таблети (с операционни системи iOS, Android) и инспекция (compliance check) на крайно клиентската машина, който се извършва по време на изграждането на защитена връзка;
REQ.54.	Системата да има възможност за надграждане с допълнителен лиценз инсталиран на защитната стена, с който да открива и управлява IoT (Internet of Things) устройства като предоставя възможност за автоматично генериране на препоръчани правила за достъп и контрол.
REQ.55.	Хардуерна гаранция за срок от минимум 5 (пет) години.
REQ.56.	Техническа поддръжка за срок от минимум 5 (пет) години.
REQ.57.	Получаване на нови версии на софтуера за срок от минимум 5 (пет) години.
REQ.58.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя.

5. Комутатор тип 2 – количество 2 броя

Технически изисквания	
REQ.1	Тип на кутията/шасито - за директен монтаж в 19" шкаф.
REQ.2	Захранване – модулно, 220 до 240 VAC с два токозахранващи модула за резервиране.
REQ.3	Работен температурен диапазон от 0º до +40 ºC.
REQ.4	Работна относителна влажност от до 90% .
REQ.5	Минимум 48 оптични порта поддържащи 1/10/25 Gbps и 6 QSFP28 порта поддържащи 40/100 Gbps.
REQ.6	Брой USB портове - минимум 1.
REQ.7	Ethernet порт за управление - минимум 1.
REQ.8	Сериен конзолен порт - минимум 1.
REQ.9	Да поддържа изолиране на потребителите от един и същ VLAN.
REQ.10	Да поддържа хардуерно реализирани листи за филтриране на трафика на база source/destination IP адреси, source/destination MAC адреси, протоколи и Layer 4 TCP/UDP номера на портове.
REQ.11	Да поддържа игнориране на BPDU пакети получавани от клиентски портове.
REQ.12	Да подържа възможност за игнориране на STP root bridge информация през неоторизирани портове.
REQ.13	Хардуерно маршуритизиране и комутиране със следните параметри, като минимум: • Производителност – 3.5 Tbps. • Forwarding – 1 200 Mpps. • Latency – под 1 микросекунда. • Брой IPv4 и IPv6 маршрута – 2 680 000.
REQ.14	MAC адреси – минимум 512 000.
REQ.15	Да поддържа Jumbo frames от поне 9198 байта.
REQ.16	Да поддържа минимум 3500 802.1Q VLAN.
REQ.17	Spanning Tree – IEEE 802.1d, 802.1w и 802.1w
REQ.18	Да поддържа следните протоколи за маршрутизация: • Статично маршрутизиране. • IGMPv2 и IGMPv3 snooping. • VRRP. • Динамично маршрутизиране: RIPv2, OSPFv2, OSPFv3 • PIM, MSDP, SSM мултикаст маршрутизация. • DHCP Relay.

REQ.19	Да поддържа Netflow или подобен протокол
REQ.20	Да има възможност за поддържка на VXLAN BGP EVPN.
REQ.21	Да поддържа IEEE 802.3ad LACP протокол.
REQ.22	Да поддържа MLAG.
REQ.23	Да поддържа LLDP и LLDP-MED.
REQ.24	Да поддържа QoS със следните функции, като минимум: • Минимум 8 изходящи пакетни опашки на всеки порт. • Групиране на трафика в трафични класове на база произволни комбинации от Layer2, Layer 3 и Layer 4 трафични параметри, 802.1p и DCSP маркировка. • Traffic policing на база Layer2, Layer 3 и Layer 4 трафични параметри, 802.1p и DCSP маркировка и приложения • Traffic policing за входящ и изходящ трафик с възможност за задаване на CIR PIR и Commited Burst параметри. • Traffic shaping на база трафични класове. • Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всяка опашка, като процент от пропускателната способност на интерфейса. • Управление на пакетните опашки чрез задаване на минимално гарантирана скорост за всяка опашка. • Поддръжка на приоритетна опашка (PQ) • Поддръжка на Weighted Tail Drop (WTD) алгоритъм за предотвратяване на задръствания.. • DSCP и 802.1p маркиране и премаркиране на трафика на база трафични политики.
REQ.25	Да поддържа минимум следните методи за управление и наблюдение: • Управление чрез конзола. • RMON • IPv4/v6 ping. • DNS • TFTP • FTP, SFTP. • NTP клиент и сървър. • SSHv2 и SNMPv3. • Възможност за добавяне на експортиране на трафична информация чрез Netflow или подобен протокол към външна система за трафичен анализ. • Конфигурация в отделен, конфигурационен, файл позволяващ бързото и лесно преместване на конфигурацията върху ново у-во. • Задаване ниво на достъп до системата за всеки администратор. • Оторизация на администраторите за достъп до всяка команда/групи от команди. • Работа с външна система за съхраняване на информация, за въведените от всеки потребител команди. • Traffic policing за контролиране на трафика до контролната система на комутатора. • Идентификация на администраторите чрез външни RADIUS и TACACS+ системи. • Обособен Ethernet порт за out of band управление и наблюдение на устройството.
REQ.26	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя.
REQ.27	Срок на хардуерната гаранция: минимум 5 (пет) години.
REQ.28	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.29	Получаване на нови версии на софтуера – минимум 5 (пет) години.

6. Комутатор тип 3 – количество 2 броя

Технически изисквания	
REQ.1	Тип на кутията/шасито - за монтаж в 19“ шкаф
REQ.2	Захранване – модулно, с минимум два токозахранващи модула за резервиране, 220-240v AC, 50Hz
REQ.3	Модулни вентилатори
REQ.4	Минимум 24 порта поддържащи 1GE, 10GE и 25GE чрез SFP, SFP+ и SFP28 модули
REQ.5	Да поддържа инсталиране на минимум 4 порта поддържащи 40GE и 100GE чрез допълнителен външен модули
REQ.6	Брой USB портове - минимум 1
REQ.7	Да поддържа изолиране на потребителите от един и същ VLAN
REQ.8	Да поддържа 802.1X на всички портове
REQ.9	Да поддържа 802.1x идентификация и оторизация с прилагането на динамични VLAN и ACL.
REQ.10	Да поддържа идентификация на база MAC адреси
REQ.11	Да поддържа идентификация чрез вграден Web портал
REQ.12	Да поддържа комбиниране на методите идентификация на един порт – 802.1x, MAC адрес, WEB идентификация.
REQ.13	Да поддържа RADIUS CoA
REQ.14	Да поддържа хардуерно реализирани листи за филтриране на трафика на база source/destination IP адреси, source/destination MAC адреси, протоколи и Layer 4 TCP/UDP номера на портове
REQ.15	Да поддържа 802.1AE 256 битово криптиране на всички портове
REQ.16	Да поддържа автоматично инспектиране на DHCP трафика със следните функции: • блокиране на DHCP заявки с разлика в MAC адреса на Ethernet фрейма и MAC адреса в DHCP заявката. • блокиране на DHCP пакети за освобождаване на адрес или отказ, които идват от порт различен от този, през който е получен IP адреса. • Защита от IP Spoofing
REQ.17	Да поддържа автоматично запаметяване на използвания от клиентското у-во MAC адрес и да блокира мрежовия достъп за други устройства свързвани към същия порт
REQ.18	Да поддържа игнориране на BPDU пакети получавани от клиентски портове
REQ.19	Да подържа възможност за игнориране на STP root bridge информация през неоторизирани портове
REQ.20	Да поддържа криптографски метод за проверка на автентичността на използвания софтуер
REQ.21	Хардуерно маршуритизиране за IPv4 и IPv6 със следните параметри, като минимум: • Производителност - 1900Gbps • Forwarding – 1480Mpps • Брой IPv4 и IPv6 маршрута – 58000 • Multicast маршрути - 8000 • SVI интерфейси - 1000 • Пакетни буфери – 16MB
REQ.22	DRAM - минимум 16GB DRAM
REQ.23	Да поддържа стекове свързване между минимум осем устройства чрез използване на стак портове с капацитет от 1Tbit
REQ.24	Да поддържа Statefull Switch Over (SSO) между комутатори в един стек за минимум следните функции: • Маршрутизиране • STP • 802.3ad

REQ.25	MAC адреси – минимум 32000
REQ.26	Да поддържа Jumbo frames от поне 9198 байта
REQ.27	Да поддържаминимум 4000 802.1Q VLAN
REQ.28	Да поддържа енкапсулация на трафика във VXLAN
REQ.29	Spanning Tree – IEEE 802.1d, 802.1w и 802.1w
REQ.30	Да поддържа следните протоколи за маршрутизация: • Статично маршрутизиране за IPv4 и IPv6 • RIPv1, RIPv2, RIP-NG • OSPFv2 и OSPFv3 • BGPv4 • IS-ISv4 • IGMPv2 и IGMPv3 snooping • Мултикас маршрутизиране с PIM-SM и PIM-SSM • Маршрутизиране на база политики • Виртуализация на машрутизиращите таблици и протоколи • VRRP
REQ.31	Да поддържа IEEE 802.3ad LACP протокол
REQ.32	Да поддържа IEEE 802.3ad групи с портове от различни комутатори в един стек
REQ.33	Да поддържа LLDP
REQ.34	Да има възможност за класифициране на трафичните потоци на ниво апликациите посредством вградена DPI система
REQ.35	Да поддържа QoS със следните функции, като минимум: • Минимум 8 изходящи пакетни опашки на всеки порт. • Групиране на трафика в трафични класове на база произволни комбинации от Layer2, Layer 3, Layer 4 и Layer 7 трафични параметри, 802.1p и DCSP маркировка • Traffic policing на база трафични класове • Traffic policing за входящ и изходящ трафик с възможност за задаване на CIR PIR и Commited Burst параметри. • Traffic shaping на база трафични класове • Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всяка опашка, като процент от пропускателната способност на интерфейса • Управление на пакетните опашки чрез задаване на минимално гарантирана скорост за всяка опашка. • Поддръжка на приоритетна опашка (PQ) • Поддръжка на Weighted Tail Drop (WTD) алгоритъм за предотвратяване на задръствания • DSCP и 802.1p маркиране и премаркиране на трафика на база трафични политики
REQ.36	Да поддържа MPLS
REQ.37	Да поддържа L2 и L3 MPLS VPN
REQ.38	Да има възможност за поддържка на BGP EVPN
REQ.39	Да поддържа работа като Multicast DNS шлюз
REQ.40	Да има възможност за изграждането на софтуерно управлявани виртуални мрежи (SDN Overlays)
REQ.41	Да има възможност за изграждане на SDN Overlay с използване на BGP EVPN, MPLS, LISP или подобен контролен протокол
REQ.42	Да поддържа динамична сегментация на потребителите на база минимум MAC адреси, профилиране на потребителското устройства и 802.1x удостоверяване на идентичност
REQ.43	Да поддържа минимум следните методи за управление и наблюдение: • Управление чрез конзола и GUI

	• RMON. • IPv4/v6 ping • DNS • TFTP • FTP • NTP клиент и сървър • SSHv2 и SNMPv3 • Експортиране на трафична информация за минимум 64000 трафични потока чрез IPFIX, Netflow, JFlow или подобен протокол към външна система за трафичен анализ • Конфигурация в отделен конфигурационен файл, който позволява бързо и лесно преместване на конфигурацията върху ново у-во • Задаване ниво на достъп до системата за всеки администратор. • Работа с външна система за съхраняване на изпълнените от всеки администратор команди • Traffic policing за контролиране на трафика до контролната система на комутатора • Идентификация на администраторите чрез външни RADIUS и TACACS+ системи. • Отделен Ethernet порт за out of band управление и наблюдение на устройството • Да поддържа NETCONF/YANG интерфейс • Да поддържа възможност за работа с контейнери • Да поддържа увеличаване на обема за съхранение на данни чрез включване на външен USB диск през минимум един USB 3.0 интерфейс • Да поддържа стрийминг на телеметрия на база YANG моделите
REQ.44	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя
REQ.45	Устройството да е окомплектовано с необходимите планки за монтаж в 19“ шкаф, стекови модули и кабели.
REQ.46	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.47	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.48	Получаване на нови версии на софтуера - минимум 5 (пет) години.

7. Комутатор тип 4 – количество 12 броя

Технически изисквания	
REQ.1	Тип на кутията/шасито - за монтаж в 19“ шкаф
REQ.2	Захранване – модулно, с минимум два токозахранващи модула за резервиране, 220-240v AC, 50Hz
REQ.3	Модулни вентилатори
REQ.4	Минимум 48 порта поддържащи 100M / 1G Base-T (RJ45) интерфейса
REQ.5	Да притежава минимум 4 порта поддържащи 1GE и 10GE чрез допълнителен външен модули
REQ.6	Брой USB портове - минимум 1
REQ.7	Да поддържа изолиране на потребителите от един и същ VLAN
REQ.8	Да поддържа 802.1X на всички портове за потребители
REQ.9	Да поддържа 802.1x идентификация и оторизация с прилагането на динамични VLAN и ACL.
REQ.10	Да поддържа идентификация на база MAC адреси
REQ.11	Да поддържа идентификация чрез вграден Web портал
REQ.12	Да поддържа комбиниране на методите идентификация на един порт – 802.1x, MAC адрес, WEB идентификация.
REQ.13	Да поддържа RADIUS CoA

REQ.14	Да поддържа хардуерно реализирани листи за филтриране на трафика на база source/destination IP адреси, source/destination MAC адреси, протоколи и Layer 4 TCP/UDP номера на портове
REQ.15	Да поддържа 802.1AE 128 битово криптиране на всички портове
REQ.16	Да поддържа автоматично инспектиране на DHCP трафика със следните функции: • блокиране на DHCP заявки с разлика в MAC адреса на Ethernet фрейма и MAC адреса в DHCP заявката. • блокиране на DHCP пакети за освобождаване на адрес или отказ, които идват от порт различен от този, през който е получен IP адреса. • Защита от IP Spoofing
REQ.17	Да поддържа автоматично запаметяване на използвания от клиентското у-во MAC адрес и да блокира мрежовия достъп за други устройства свързвани към същия порт
REQ.18	Да поддържа игнориране на BPDU пакети получавани от клиентски портове
REQ.19	Да подържа възможност за игнориране на STP root bridge информация през неоторизирани портове
REQ.20	Да поддържа криптографски метод за проверка на автентичността на използвания софтуер
REQ.21	Хардуерно маршуритизиране за IPv4 и IPv6 със следните параметри, като минимум: • Производителност - 170Gbps • Forwarding – 130Mpps • Брой IPv4 и IPv6 маршрута – 6000 • Multicast маршрути - 1000 • SVI интерфейси - 1000 • Пакетни буфери – 6MB
REQ.22	DRAM - минимум 4GB DRAM
REQ.23	Да поддържа стекове свързване между минимум осем устройства чрез използване на стак портове с капацитет от 160Gbit
REQ.24	Да поддържа Statefull Switch Over (SSO) между комутатори в един стек за минимум следните функции: • Маршрутизиране • STP • 802.3ad
REQ.25	MAC адреси – минимум 32000
REQ.26	Да поддържа Jumbo frames от поне 9198 байта
REQ.27	Да има възможност за поддържка на енкапсулация на трафика във VXLAN
REQ.28	Spanning Tree – IEEE 802.1d, 802.1w и 802.1w
REQ.29	Да поддържа следните протоколи за маршрутизация: • Статично маршрутизиране за IPv4 и IPv6 • OSPFv2 и OSPFv3 • IS-ISv4 • IGMPv2 и IGMPv3 snooping • Мултикас маршрутизиране с PIM-SM и PIM-SSM • Маршрутизиране на база политики • Виртуализация на машрутизиращите таблици и протоколи • VRRP
REQ.30	Да поддържа IEEE 802.3ad LACP протокол
REQ.31	Да поддържа IEEE 802.3ad групи с портове от различни комутатори в един стек
REQ.32	Да поддържа LLDP
REQ.33	Да има възможност за класифициране на трафичните потоци на ниво апликациите посредством вградена DPI система
REQ.34	Да поддържа QoS със следните функции, като минимум:

	• Минимум 8 изходящи пакетни опашки на всеки порт. • Групиране на трафика в трафични класове на база произволни комбинации от Layer2, Layer 3, Layer 4 и Layer 7 трафични параметри, 802.1p и DCSP маркировка • Traffic policing на база трафични класове • Traffic policing за входящ и изходящ трафик с възможност за задаване на CIR PIR и Commited Burst параметри. • Traffic shaping на база трафични класове • Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всяка опашка, като процент от пропускателната способност на интерфейса • Управление на пакетните опашки чрез задаване на минимално гарантирана скорост за всяка опашка. • Поддръжка на приоритетна опашка (PQ) • Поддръжка на Weighted Tail Drop (WTD) алгоритъм за предотвратяване на задръствания • DSCP и 802.1p маркиране и премаркиране на трафика на база трафични политики
REQ.35	Да поддържа изграждането на софтуерно управлявани виртуални мрежи
REQ.36	Да поддържа динамична сегментация на потребителите на база минимум MAC адреси, профилиране на потребителското устройства и 802.1x удостоверяване на идентичност
REQ.37	Да поддържа минимум следните методи за управление и наблюдение: • Управление чрез конзола и GUI • RMON. • IPv4/v6 ping • DNS • TFTP • FTP • NTP клиент и сървър • SSHv2 и SNMPv3 • Експортиране на трафична информация за минимум 16000 трафични потока чрез IPFIX, Netflow, JFlow или подобен протокол към външна система за трафичен анализ • Конфигурация в отделен конфигурационен файл, който позволява бързо и лесно преместване на конфигурацията върху ново у-во • Задаване ниво на достъп до системата за всеки администратор. • Работа с външна система за съхраняване на изпълнените от всеки администратор команди • Traffic policing за контролиране на трафика до контролната система на комутатора • Идентификация на администраторите чрез външни RADIUS и TACACS+ системи. • Отделен Ethernet порт за out of band управление и наблюдение на устройството • Да поддържа NETCONF/YANG интерфейс • Да поддържа стрийминг на телеметрия на база YANG моделите
REQ.38	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя
REQ.39	Устройството да е окомплектовано с необходимите планки за монтаж в 19“ шкаф, външни интерфейсни модули и кабели.
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.

8. Комутатор тип 5 – количество 6 броя

Технически изисквания	
REQ.1	Тип на кутията/шасито - за монтаж в 19“ шкаф
REQ.2	Захранване – модулно, с минимум два токозахранващи модула за резервиране, 220-240v AC, 50Hz
REQ.3	Модулни вентилатори
REQ.4	Минимум 48 порта поддържащи 100M / 1G Base-T интерфейса
REQ.5	Да притежава минимум 8 порта поддържащи 1GE и 10GE чрез допълнителен външен модули
REQ.6	Брой USB портове - минимум 1
REQ.7	Да поддържа изолиране на потребителите от един и същ VLAN
REQ.8	Да поддържа 802.1X на всички портове
REQ.9	Да поддържа 802.1x идентификация и оторизация с прилагането на динамични VLAN и ACL.
REQ.10	Да поддържа идентификация на база MAC адреси
REQ.11	Да поддържа идентификация чрез вграден Web портал
REQ.12	Да поддържа комбиниране на методите идентификация на един порт – 802.1x, MAC адрес, WEB идентификация.
REQ.13	Да поддържа RADIUS CoA
REQ.14	Да поддържа хардуерно реализирани листи за филтриране на трафика на база source/destination IP адреси, source/destination MAC адреси, протоколи и Layer 4 TCP/UDP номера на портове
REQ.15	Да поддържа 802.1AE 256 битово криптиране на всички портове
REQ.16	Да поддържа автоматично инспектиране на DHCP трафика със следните функции: • блокиране на DHCP заявки с разлика в MAC адреса на Ethernet фрейма и MAC адреса в DHCP заявката. • блокиране на DHCP пакети за освобождаване на адрес или отказ, които идват от порт различен от този, през който е получен IP адреса. • Защита от IP Spoofing
REQ.17	Да поддържа автоматично запаметяване на използвания от клиентското у-во MAC адрес и да блокира мрежовия достъп за други устройства свързвани към същия порт
REQ.18	Да поддържа игнориране на BPDU пакети получавани от клиентски портове
REQ.19	Да подържа възможност за игнориране на STP root bridge информация през неоторизирани портове
REQ.20	Да поддържа криптографски метод за проверка на автентичността на използвания софтуер
REQ.21	Хардуерно маршуритизиране за IPv4 и IPv6 със следните параметри, като минимум: • Производителност - 250Gbps • Forwarding – 190Mpps • Брой IPv4 и IPv6 маршрута – 48000 • Multicast маршрути - 8000 • SVI интерфейси - 1000 • Пакетни буфери – 16MB
REQ.22	DRAM - минимум 8GB DRAM
REQ.23	Да поддържа стекове свързване между минимум осем устройства чрез използване на стак портове с капацитет от 480Gbit
REQ.24	Да поддържа Statefull Switch Over (SSO) между комутатори в един стек за минимум следните функции: • Маршрутизиране • STP • 802.3ad
REQ.25	MAC адреси – минимум 32000
REQ.26	Да поддържа Jumbo frames от поне 9198 байта

REQ.27	Да поддържа минимум 4000 802.1Q VLAN
REQ.28	Да поддържа енкапсулация на трафика във VXLAN
REQ.29	Spanning Tree – IEEE 802.1d, 802.1w и 802.1w
REQ.30	Да поддържа следните протоколи за маршрутизация: • Статично маршрутизиране за IPv4 и IPv6 • RIPv1, RIPv2, RIP-NG • OSPFv2 и OSPFv3 • BGPv4 • IS-ISv4 • IGMPv2 и IGMPv3 snooping • Мултикас маршрутизиране с PIM-SM и PIM-SSM • Маршрутизиране на база политики • Виртуализация на машрутизиращите таблици и протоколи • VRRP
REQ.31	Да поддържа IEEE 802.3ad LACP протокол
REQ.32	Да поддържа IEEE 802.3ad групи с портове от различни комутатори в един стек
REQ.33	Да поддържа LLDP
REQ.34	Да има възможност за класифициране на трафичните потоци на ниво апликациите посредством вградена DPI система
REQ.35	Да поддържа QoS със следните функции, като минимум: • Минимум 8 изходящи пакетни опашки на всеки порт. • Групиране на трафика в трафични класове на база произволни комбинации от Layer2, Layer 3, Layer 4 и Layer 7 трафични параметри, 802.1p и DCSP маркировка • Traffic policing на база трафични класове • Traffic policing за входящ и изходящ трафик с възможност за задаване на CIR PIR и Commited Burst параметри. • Traffic shaping на база трафични класове • Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всяка опашка, като процент от пропускателната способност на интерфейса • Управление на пакетните опашки чрез задаване на минимално гарантирана скорост за всяка опашка. • Поддръжка на приоритетна опашка (PQ) • Поддръжка на Weighted Tail Drop (WTD) алгоритъм за предотвратяване на задръствания • DSCP и 802.1p маркиране и премаркиране на трафика на база трафични политики
REQ.36	Да поддържа MPLS
REQ.37	Да поддържа L2 и L3 MPLS VPN
REQ.38	Да има възможност за поддържка на BGP EVPN
REQ.39	Да поддържа работа като Multicast DNS шлюз
REQ.40	Да има възможност за поддържка за изграждането на софтуерно управлявани виртуални мрежи (SDN Overlays)
REQ.41	Да има възможност за поддържка за изграждането на SDN Overlay с използване на BGP EVPN, MPLS, LISP или подобен контролен протокол
REQ.42	Да поддържа динамична сегментация на потребителите на база минимум MAC адреси, профилиране на потребителското устройства и 802.1x удостоверяване на идентичност
REQ.43	Да поддържа минимум следните методи за управление и наблюдение: • Управление чрез конзола и GUI • RMON. • IPv4/v6 ping

	• DNS • TFTP • FTP • NTP клиент и сървър • SSHv2 и SNMPv3 • Експортиране на трафична информация за минимум 64000 трафични потока чрез IPFIX, Netflow, JFlow или подобен протокол към външна система за трафичен анализ • Конфигурация в отделен конфигурационен файл, който позволява бързо и лесно преместване на конфигурацията върху ново у-во • Задаване ниво на достъп до системата за всеки администратор. • Работа с външна система за съхраняване на изпълнените от всеки администратор команди • Traffic policing за контролиране на трафика до контролната система на комутатора • Идентификация на администраторите чрез външни RADIUS и TACACS+ системи. • Отделен Ethernet порт за out of band управление и наблюдение на устройството • Да поддържа NETCONF/YANG интерфейс • Да поддържа възможност за работа с контейнери • Да поддържа увеличаване на обема за съхранение на данни чрез включване на външен USB диск през минимум един USB 3.0 интерфейс • Да поддържа стрийминг на телеметрия на база YANG моделите
REQ.44	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя
REQ.45	Устройството да е окомплектовано с необходимите планки за монтаж в 19“ шкаф, стекови модули, външни интерфейсни модули и кабели.
REQ.46	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.47	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.48	Получаване на нови версии на софтуера - минимум 5 (пет) години.

9. Мрежови интерфейсен модул за налични комутатори – количество 2 броя

Технически изисквания	
REQ.1	Интерфейсен модул за съществуващи комутатори Catalyst 9300
REQ.2	Осем порта за 10GE SFP модули.

10. 10GE оптичен DAC кабел с дължина 10м – количество 4 броя

Технически изисквания	
REQ.1	10GE оптичен DAC кабел с дължина 10м и SFP+ интерфейси.
REQ.2	Кабелът трябва да бъде от същия производител, както предложените комутатори, или да бъде сертифициран за използване от него.

11. 10GE оптичен DAC кабел с дължина 5м – количество 6 броя

Технически изисквания	
REQ.1	10GE оптичен DAC кабел с дължина 5м и SFP+ интерфейси.
REQ.2	Кабелът трябва да бъде от същия производител, както предложените комутатори, или да бъде сертифициран за използване от него.

12. 10GE оптичен DAC кабел с дължина 1м – количество 18 броя

Технически изисквания	
REQ.1	10GE оптичен DAC кабел с дължина 1м и SFP+ интерфейси.
REQ.2	Кабелът трябва да бъде от същия производител, както предложените комутатори, или да бъде сертифициран за използване от него.

13. 100GBASE-CR4 пасивен меден кабел с дължина 1м и QSFP+ интерфейси – количество 2 броя

Изискано от Възложителя	
REQ.1	100GBASE-CR4 пасивен меден кабел с дължина 1м и QSFP+ интерфейси.
REQ.2	Кабелът трябва да бъде от същия производител, както предложените комутатори, или да бъде сертифициран за използване от него.

14. 10GBASE SFP+ модул мултимоден – количество 40 броя

Технически изисквания	
REQ.1	10GBASE-SR SFP+ модул.
REQ.2	Конектор – дуплексен LC.
REQ.3	Модулът трябва да бъде от същия производител, както предложените комутатори, или да бъде сертифициран за използване от него.

15. 1000BASE-T SFP модул – количество 10 броя

Технически изисквания	
REQ.1	1000BASE-T SFP модул.
REQ.2	Конектор – RJ-45.

REQ.3	Модулът трябва да бъде от същия производител, както предложените комутатори, или да бъде сертифициран за използване от него.

16. Маршрутизатор тип 1 – количество 2 броя

Технически изисквания	
REQ.1	Захранване – 220 до 240 VAC.
REQ.2	Монтаж в 19“ шкаф.
REQ.3	Два интерфейса 1000BASE-T.
REQ.4	Два порта SFP.
REQ.5	Брой USB 3.0 интерфейси – 1.
REQ.6	Конзолен интерфейс – 1.
REQ.7	Възможност за добавяне на външен 8 портове модул, както и външен LTE модул
REQ.8	Пропускателна способност до 1Gbps за IPSec с 1400 байта или по-големи пакети. Производителността на предлаганото устройство трябва да бъде удостоверена чрез брошура, техническо ръководство или декларация от производителя.
REQ.9	DRAM – 8GB.
REQ.10	Поддържа IPv4 и IPv6 WAN транспортни мрежи.
REQ.11	Поддръжка на IPSec, GRE, PPP, LISP протокол.
REQ.12	AES-256 GCM алгоритъм за криптиране на трафика.
REQ.13	Изграждане на стандартни IPsec/IKEv2 тунели до устройства на други производители.
REQ.14	Изграждане на GRE тунели до външни системи за сигурност.
REQ.15	Поддръжка на GRE over IPSec.
REQ.16	Поддръжка на 4000 листи за достъп
REQ.17	Поддръжка на 1 600 000 IPv4 пътища
REQ.18	Поддръжка на мултикаст Protocol Independent Multicast Sparse Mode (PIM SM), PIM Source-Specific Multicast (SSM)
REQ.19	Използване на сертификати от вътрешно CA
REQ.20	Инсталиран от производителя цифров сертификат в TPM или еквивалентен модул.
REQ.21	Поддръжка на изолиране на трафика и маршрутизиращите таблици (до 4000) чрез използване на VRF, VRF Lite или еквивалентен метод за сегментация.
REQ.22	Поддръжка на рутиране на база политики
REQ.23	Поддръжка на SIP, RSVP, SRST протоколи
REQ.24	Рутинг протоколи: OSPF BGP IS-IS

Технически изисквания	
	VRRP
REQ.25	Вградено разпознаване на приложения.
REQ.26	Филтриране на трафика чрез ACL.
REQ.27	802.1Q VLAN.
REQ.28	Поддръжка на 1M NAT транслации.
REQ.29	Протоколи и методи за управление и наблюдение: DHCP клиент. DHCP сървър. DNS. NTP. SNMP. SSH. Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow или еквивалентен протокол към външна система за анализ на трафика. Автоматично откриване на WAN MTU. Управление на достъпа чрез RADIUS и TACACS+ системи.
REQ.30	QoS: 8 пакетни опашки на интерфейс. LLQ опашка. Управление на пакетните опашки с WRP или еквивалентен алгоритъм. Управление на задръстванията с WRED или еквивалентен алгоритъм. Traffic policing. Traffic shaping. QoS върху VLAN интерфейси. QoS: 8 пакетни опашки на интерфейс. LLQ опашка. Управление на пакетните опашки с WRP или еквивалентен алгоритъм. Управление на задръстванията с WRED или еквивалентен алгоритъм. Traffic policing. Traffic shaping. QoS върху VLAN интерфейси. QoS на ниво тунел.
REQ.31	Планки за монтаж в 19“ шкаф, захранващ кабел.
REQ.32	Хардуерна гаранция за срок от минимум 5 (пет) години.
REQ.33	Техническа поддръжка за срок от минимум 5 (пет) години.
REQ.34	Получаване на нови версии на софтуера за срок от минимум 5 (пет) години.
REQ.35	Лицензни абонаменти за използване на софтуерни функции за срок от минимум 5 (пет) години.

17. Система за защита на електронна поща – количество 2 броя

Технически изисквания	
REQ.1	Да извършва последователна проверка на входящи и изходящи email съобщения с различни системи и методи: DKIM и SFP проверка. Филтриране на входящи съобщения на база нивото на репутация на изпращача. Защита против спам с възможност за пропускане, унищожаване, връщане или поставяне на съобщението под карантина. Антивирусна защита. Graymail защита с принудително отстраняване на URL линка за отписване. Подправени съобщения
REQ.2	Да поддържа създаването на политики за прилагане на следните действия върху email съобщенията – пропускане, унищожаване, връщане обратно, поставяне на карантина.
REQ.3	Да поддържа лимитиране броя на изходящите съобщения за всеки потребител.
REQ.4	Да има възможност за поддържка на вградена DLP система.
REQ.5	Да поддържа интеграция с външна DLP система.
REQ.6	Да поддържа задължително прилагане на договорено TLS шифроване за групи от изпращачи. При получаване на нешифровано съобщение от тези групи, системата трябва да може да върне автоматичен мейл със съобщение, че се използва нешифрована комуникация.
REQ.7	Да има възможност за Envelop Encryption.
REQ.8	Да поддържа S/MIME шифроване.
REQ.9	Да поддържа създаването на политики и правила за филтриране.
REQ.10	Функционалност за локална карантина.
REQ.11	Функционалност за одитни записи.
REQ.12	Функционалност за доклади.
REQ.13	Да поддържа минимум следните методи за управление и наблюдение: Web базиран графичен интерфейс HTTP и HTTPS Ping DNS FTP NTP SSHv2 WEB API за интеграция с външни системи. Вградена система за изготвяне на отчети.
REQ.14	Софтуерът да е окомплектован със съответните лицензи и права за използване според условията на производителя за минимум 650 потребителя.
REQ.15	Възможност за инсталиране върху виртуални или хардуерни аплайънси или сървъри, съгласно изискванията на производителя.
REQ.16	Ако предложението на участник включва сървъри, то те трябва да се доставят с всички необходими лицензи за операционни системи, бази данни и допълнителен софтуер, съгласно изискванията на производителя.

Технически изисквания	
REQ.17	Да поддържа инсталиране върху виртуалните аплайънси съвместими с VMWare ESXi инфраструктура.
REQ.18	Техническа поддръжка за срок от минимум 5 (пет) години.
REQ.19	Получаване на нови версии на софтуера за срок от минимум 5 (пет) години.
REQ.20	Лицензни абонаменти за използване на софтуерни функции за срок от минимум 5 (пет) години.

18. Endpoint Security – мрежова сигурност потребители

Технически изисквания	
REQ.1	Участникът трябва да достави всички необходими лицензи с права за ползване на всички изисквани функционалности за защита на 650 работни станции и сървъри, за период от минимум 60 (шестдесет) месеца.
REQ.2	Антивирусни функционалности от следващо поколение базирани на машинно обучение, локален анализ и предотвратяване на заплахи
REQ.3	Предотвратяване на заплахи, базирано на поведение и динамичен анализ на работещи процеси
REQ.4	Предотвратяване на експлоатация чрез техника на експлоатиране
REQ.5	Автоматизирана интеграция с базирана в облак услуга за предотвратяване на злонамерен софтуер, с отчети за анализ и поддръжка на минимум 100MB размера на файла
REQ.6	Модул за инспекция на мрежата с цел спиране на мрежови атаки
REQ.7	Функционалност за създаване на профили за сигурност и задаване на изключения
REQ.8	Извънредно и планирано сканиране на крайни точки
REQ.9	Защита срещу злонамерен софтуер, крипто вируси и атаки без файлове
REQ.10	Унифициран олекотен агент за защита, откриване и реакция срещу заплахи на крайните точки
REQ.11	Защитна стена на хоста
REQ.12	Криптиране на диска
REQ.13	Управление на USB устройства
REQ.14	Персонализирани правила за превенция
REQ.15	Автоматично групиране на свързани сигнали от различни източници в един инцидент
REQ.16	Интуитивен изглед на инцидента с преглед на инцидента и тактики на MITRE и ключова информация за инцидента.
REQ.17	Възможност за персонализирано оценяване на инциденти
REQ.18	Списък на забележителни артефакти от сигнали и обогатена информация от услуга за разузнаване за заплахи
REQ.19	Изброяване на потребители и хостове, участващи в инциденти, за бързо определяне на обхвата на инцидента
REQ.20	Функционалност за възлагане на конкретни инциденти на членовете на екипа
REQ.21	Функционалност за добавяне на коментари към инциденти
REQ.22	Обединяване на инциденти по избор

REQ.23	Функционалност за отдалечен терминал
REQ.24	Функционалност за изпълнение на команди и скриптове на CMD, PowerShell и Python в Windows
REQ.25	Функционалност за изпълнение на команди на Bash и Python на macOS и Linux
REQ.26	Отдалечено изолиране на единична крайна точка или множество крайни точки
REQ.27	Отдалечено изтриване на файл на една или няколко крайни точки
REQ.28	Функционалност за преглеждане, спиране или прекратяване на работещи процеси или изтегляне на двоични файлове с графичен мениджър на задачи за Windows, macOS и Linux
REQ.29	Мащабируемо, базирано на облак управление, както и инсталиране на агент
REQ.30	Единна уеб-базирана конзола за управление за сигурността на крайните точки, както и разширено откриване и реакция
REQ.31	Контрол на достъпа, базиран на роли (RBAC) за персонализирани права
REQ.32	Възможност за достъп до платформата посредством мултифакторна автентикация (MFA)
REQ.33	Персонализирани информационни табла за високо ниво на сигурност и оперативна информация
REQ.34	Инструменти за управление на трети страни базирани на стандарти приложно програмни интерфейси, които се интегрират и извършват административни действия
REQ.35	Решението да включва права за използване на облачна среда за съхранение и анализиране на логове от крайни устройства и защитни стени с капацитет минимум 200 GB на ден и 30 дневен период за съхранение.
REQ.36	Агента на решението да може да бъде инсталиран на минимум: ●Windows XP SP3 и по-нови ● Windows 7 и по-нови ● Windows Server 2003 R2 ● Windows Server 2008 и по-нови ● ORACLE 6, 7, 8, 9 ● Debian 9,10,11 ● RedHat 6, 7, 8, 9 ● Ubuntu ● Android 5 и по-нови ● macOS ● iOS ● VMware AppVolumes ● VMware Horizon View ● VMware ThinApp
REQ.37	Сертификация на производителя по ISO 27001
REQ.38	Автоматизирано свързване на данни от крайни точки, мрежа, облак и данни за самоличност, включително предупреждения и събития за сигурност
REQ.39	Автоматизиран анализ на първопричината за всеки сигнал, включително мрежови сигнали, ако има налични данни за крайната точка
REQ.40	Да има възможност за предоставяне на анализа във времева линия, за да може да се видят всички действия и сигнали и тяхната последователност
REQ.41	Възможност за използване на база за разузнаване (Threat Intelligence) на заплахи от източници на трети страни във формати JSON и CSV
REQ.42	Откриване и отговор на заплахи, включващи управлявани и неуправлявани крайни точки

REQ.43	Откриване и реагиране на заплахи, включващи облачни сървъри
REQ.44	Непрекъснато събиране и централизирано съхранение на всички данни за сигурност с цел поведенчески анализи
REQ.45	Решението да прави анализ на крайните устройства включително инвентаризация, оценка и управление на уязвимости, както и незабавно намиране и премахване на заплахи
REQ.46	Възможност за разширение времето за съхранение на логове от крайните машини с допълнителен лиценз за период не по-малък от 5 години
REQ.47	Една година съхранение на одитни дневници на административна и следствена дейност
REQ.48	Решението да включва следните разширени функционалности за събиране, задълбочен анализ и разследване на данни за 100 броя Windows базирани машини: ● История на браузъра (Chrome, Edge, Firefox, Internet Explorer) ● Достъп до файлове ● Стартиране на процеси ● Мрежова активност ● История на команди ● Отдалечен достъп
REQ.49	Участникът трябва да осигури техническа поддръжка от производителя за целия срок на предоставеното право на ползване;
REQ.50	Поддръжката да включва права за ползване на софтуерни обновления, софтуер за корекции на грешки и помощ при отстраняване на несъвместимости с документираното поведение на софтуерното решение;

19. Система за динамичен анализ на зловреден код и защита от кибератаки на електронни email съобщения

Технически изисквания	
REQ.1	Тип решение: 2 броя хардуер (High-Availability) с вграден софтуер и минимум 5-годишна поддръжка, както и минимум 5-годишен абонамент за прилежащи услуги към хардуерните устройства за 650 потребителя
REQ.2	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.3	Решението трябва да се предоставя под формата на специализиран хардуер, като производителят 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.4	Решението трябва да притежава следните сертификати: Federal Information Processing Standards (FIPS) 140-2 и Common Criteria (CC).
REQ.5	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 компрометиране на системите на организацията.
REQ.6	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.7	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.8	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.9	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.10	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.11	Решението трябва да може да извлича и анализира вмъкнати файлове в документи, като например pdf, rtf или MS Office документи.
REQ.12	Решението трябва да може да поставя в карантина и да алармира за криптирани MS Office документи.
REQ.13	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.14	Решението трябва да може да поставя в карантина и да алармира за електронни съобщения, които съдържат в себе си съкратени URL адреси.
REQ.15	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.16	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.17	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.18	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.19	Решението трябва да може да анализира URL адреси от тип ftp, http и https.
REQ.20	Решението трябва да може да анализира base64 кодирани URL адреси.
REQ.21	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.22	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.23	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.24	Решението трябва да може да анализира (във виртуалните машини за динамичен анализ) сваленте 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.25	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.26	По време на анализа във виртуалните машини решението трябва да може да извлича и анализира URL адресите в паметта на машините.
REQ.27	Решението трябва да може да засича ransomware криптиращи атаки и атаки, предназначени за POS терминали.
REQ.28	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.29	Решението трябва да предоставя цялостна информация след анализ на зловреден код. Информацията трябва да включва използвани уеб линкове за атаката, хеш суми на сваленте 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.
REQ.30	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.31	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.32	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.33	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.34	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.35	Решението трябва да може да прави анализ на входящи електронни съобщения, използвайки едновременно множество виртуални машини с различни операционни системи, като например минимално Windows 7 или Mac OSX, с различни версии на Service Pack, на 32 и на 64 битови платформи.

REQ.36	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.
REQ.37	Решението трябва да използва собствен, специално изграден хипервайзор.
REQ.38	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.39	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.40	Email решението трябва да поддържа inline MTA режим на работа.
REQ.41	Email решението трябва да поддържа SPAN/TAP режим на работа.
REQ.42	Email решението трябва да поддържа BCC режим на работа.
REQ.43	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.44	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.
REQ.45	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.46	Цялостният анализ на електронно съобщение не трябва да отнема повече от 10 минути.
REQ.47	Решението трябва да позволява на администраторите да конфигурират максималното време за анализ на електронните съобщения.
REQ.48	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.49	Решението трябва да може да засича и отчита опити за мрежова комуникация с Интернет от виртуалните машини по време на анализа.
REQ.50	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.51	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.52	Решението трябва да може да изпраща автоматични известия чрез Syslog, HTTP, SNMP и SMTP протоколи.
REQ.53	Решението трябва да поддържа криптирана TLS комуникация (opportunistic или imposed), за да се запази конфиденциалността на електронните съобщения.
REQ.54	Решението трябва да може да изпраща автоматични известия когато блокира или постави в карантина дадено електронно email съобщение.
REQ.55	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.56	Решението трябва да позволява използването на прокси с оторизация за свързване със сървър за обновления на софтуера и информацията за нови заплахи.
REQ.57	Решението трябва да позволява администрация чрез уеб-базирана конзола, без да се изисква инсталирането на допълнителен софтуер за достъпването ѝ.
REQ.58	Решението трябва да позволява конфигурирането на ACL списъци, за да се ограничи достъпа до интерфейса за централизирано управление.
REQ.59	Решението трябва да използва криптирана комуникация между администраторите и конзолата за централизирано управление. Трябва да позволява вмъкването на собствени дигитални сертификати на организацията.
REQ.60	Решението трябва да позволява локално конфигуриране или чрез синхронизация с NTP сървър на използваните време и часова зона.
REQ.61	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 се задава кои отчети, аларми и информация могат да виждат в конзолата за управление.
REQ.62	Решението трябва да поддържа LDAP, TACACS + или RADIUS методи за вписване на потребителите.
REQ.63	Решението трябва да може да изпраща известия за собственото си здраве и процеси и генерираните отчети, чрез SMTP, SNMP и Syslog протоколи.
REQ.64	Решението трябва да позволява извличането на аларми и отчети за активност на зловреден код в PDF формат.
REQ.65	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.66	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.67	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.68	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.
REQ.69	Устройството да може да анализира до 600 уникални прикачени файлове към email съобщения в час
REQ.70	Устройството да може да анализира прикачени файлове и URL адреси в email съобщенията за 650 потребителя
REQ.71	Устройството да е с максимална големина 1RU
REQ.72	Устройството да разполага минимално със следните портове за наблюдение на мрежата: 2x 1GigE BaseT
REQ.73	Допълнителни портове: 2x 1GigE BaseT портове за управление, сериен порт, 4x Type A USB, IPMI, VGA
REQ.74	Резервирано захранване – 1+1
REQ.75	Хардуерната гаранция за срок от минимум 5 (пет) години.
REQ.76	Техническа поддръжка за срок от минимум 5 (пет) години.
REQ.77	Получаване на нови версии на софтуера за срок от минимум 5 (пет) години.
REQ.78	Обновяване на дефиниции и сигнатури за срок от минимум 5 (пет) години

20. Система (софтуер) за одит на промените в ИКТ средите

	Технически изисквания
REQ.1	Тип решение: софтуер
REQ.2	Тип лиценз: абонамент, с включени 60 месеца поддръжка
REQ.3	Брой лицензи: за 650 потребителски акаунти/пощенски кутии и за 150 мрежови устройства
REQ.4	Да работи без да използва агенти, така че да не влияе негативно на производителността на системите и да не спира работния процес.
REQ.5	Да не се използват никакви недокументирани методи за събиране на данни от системите на организацията, тъй като подобни методи могат да доведат до отказване на поддръжка от Microsoft или от други ключови производители.
REQ.6	Да събира сурови машинни данни и да ги преобразува в опростена, ясна информация за всяко потребителско действие, за да се улесни вземането на правилни решения от организацията.
REQ.7	Да обединява данни от множество източници (логове за събития, извадки от настройките на средите, записи на действията, свързани с промени и т.н.), за да се извлече възможно най-пълната и надеждна одитна информация, без пропуски.
REQ.8	Да събира и предоставя пълни детайли за всяка промяна и опит за достъп, включително кога и къде промяната или опита за достъп са направени, кой ги е направил и какво точно е променено или достъпено.
REQ.9	Да извършва цялостно сравнение и да събира стойностите преди и след промяната за всички променени обекти.
REQ.10	Да ползва система за съхранение на данни на две нива (SQL база от данни за отчитане и файлово-базирана система за архивиране на данни в компресиран формат за дълготрайно съхранение). Този архив трябва да съдържа цялостна одитна информация за до повече от 10 години, без да намалява производителността на системата, като трябва да осигурява лесен достъп до данните за целият период.
REQ.11	Да събира одитна информация от локални и от облачни приложения и да ги съхранява в защитен, централизиран архив, което да позволява използването на общи аларми, търсене, отчитане и анализ на рисковете по сигурността
REQ.12	За активната директория (Active Directory) и груповите политики: • Да докладва за промени в активната директория и в груповите политики • Да събира информация за промените във времето на активната директория и на груповите политики, включително за участниците в групи с множество домейни и различни права на достъп • Да одитира вписванията • Да поддържа доверени и недоверени домейни
REQ.13	За MS Exchange: • Да събира информация за промените на конфигурациите в Exchange Server, Exchange databases, mailboxes, mailbox делегиранията и разрешенията. • Одитиране на достъпа до пощенски кутии без потребител • Поддръжка на Exchange 2016
REQ.14	Windows File Servers • Да докладва за промени по файлове, папки, споделени пространства и права за достъп • Да докладва за преместени, преименувани или копирани файлове

	Технически изисквания
	• Да дава информация за успешни и неуспешни опити за прочитане на данни • Да дава информация за промените във времето на ефективните права за достъп, включително и кои потребители имат превишени права за достъп • Да създава отчети за собствеността на данните, използването на данните и обема на данните, отдавна неизползвани файлове и дублирани файлове • Да докладва за чувствителни данни, включително къде са разположени, кой има активни права да ги достъпва и кой е собственик на данните, както и за успешни и неуспешни опити за достъп до данните и опити за промяна на правата за достъп до тях • Да поддържа множество файлови сървъри и файлови устройства, разположени в няколко физически обекта, домейна и организации
REQ.15	За мрежови устройства • Да докладва за промени по конфигурациите на мрежовите устройства на организацията • Да докладва за успешни и неуспешни опити за вписване в мрежовите устройства, директно или чрез VPN свързване • Да докладва за сканирани заплахи от мрежовите устройства • Да докладва за хардуерни неизправности на мрежовите устройства • Да се поддържат минимално следните видове мрежови устройства: Fortinet FortiGate, Cisco ASA, Cisco IOS, Palo Alto, SonicWall, Juniper
REQ.16	За SQL Server • Да докладва за промени по правата за достъп до SQL Server, по сървърните инстанции, по потребителските роли в тях, по базите от данни, по конкретни таблици, колони, съхранени процедури и т.н. • Да докладва за промени по съдържанието на базите от данни • Да докладва за вписванията в базите от данни (успешни и неуспешни) • Да се поддържа SQL Server 2016
REQ.17	Windows Server • Да докладва за промени по настройките на сървъра — хардуер и софтуер, услуги, приложения, мрежови настройки, настройки на регистри, DNS, файлови дялове и други • Да предоставя информация за промените по локалните политики за одитиране, неизправностите в Windows услугите, принудителните спирания на системите и промените по настройките за време • Да предоставя информация за промените във времето на настройките на Windows сървърите, включително име и версия на операционната система, статус на антивирусната система, файловите дялове, локалните потребители и групи, услугите и инсталираните програми
REQ.18	а включва предварително зададени одитни отчети и dashboard-ове, които предоставят детайлна информация за промени, опити за достъп и настройки, представени в четим вид, позволявайки на потребителите да филтрират, сортират и извличат одитните данни.
REQ.19	Да позволява на потребителите лесно да изградят собствен отчет, базиран на конкретни изисквания, включително отчети, които да обхващат множество, разнообразни системи.
REQ.20	Автоматично да изпраща отчети до зададени получатели по email или да ги запазва в споделен файлов дял по зададен график (веднъж дневно, седмично, т.н.).
REQ.21	Да поддържа извличането на отчети в няколко различни формата, включително PDF, XLS(X), DOC(X) и CSV.

	Технически изисквания
REQ.22	Да позволява на потребителите лесно да сортират и филтрират одитната информация чрез Google-подобна интерактивна търсачка, така че те лесно да открият точните данни, които са им необходими.
REQ.23	Да показва настоящите настройки на одитираните среди или как са изглеждали настройките в даден отрязък от миналото, включително активните права за достъп на даден потребител или обект, настройките на груповите политики и детайлите за настройките на Windows сървърите.
REQ.24	Да включва готови за ползване отчети, които са пригодени за проверяване на съвместимост със стандарти като ISO/IEC 27001, GDPR, PCI DSS, HIPAA, SOX, GLBA, FISMA/NIST800-53, CJIS, FERPA, NERC CIP и др.
REQ.25	Да известява чрез email или чрез SMS съобщение отговорните екипи за подозрително поведение или събития, които могат да прерастнат в инциденти по сигурността, включително активност, която надвишава изчислените норми (аларми на базата на повторяемост на едно и също събитие).
REQ.26	Да може да докладва чрез SQL SRS, да може да използва отчетните услуги на SQL сървъра по индустриален стандарт (да поддържа и безплатната версия SQL Express), за да се предоставя широка гама от одитни отчети.
REQ.27	Да притежава Dashboard-ове за оценяване на ИТ рисковете, които да позволяват на потребителите да идентифицират и оценят рисковете по три ключови показателя: управление на акаунти, права за достъп до системите за сигурност и управление на данни.
REQ.28	Да притежава Dashboard за откриване на аномално поведение, чрез който да се подобрява засичането на зловредни акаунти в ИТ средата, като предоставя агрегирани данни за аномалното потребителско поведение и да поставя съответна оценка на риска.
REQ.29	Да предоставя отчети за потребителско поведение и за анализиране на пропуските в системите за наблюдение. Да предоставя информация за потенциални инциденти, свързани със сигурността, като например действия извън нормалните бизнес часове на деня, необичайни вписвания в системите, голям брой неуспешни опити за действия, достъпване на архивирани данни, действия от досега неактивни потребителски акаунти и наличие на потенциално опасни файлове на файловите сървъри.
REQ.30	Да има управление на Event logs: Автоматично да се събират, обединяват и архивират данните за настъпили събития, така че администраторите да могат да одитират събития от общ характер, събития, свързани с услуги, вписвания на потребители и състояли се сесии с отдалечен достъп.
REQ.31	Да има Dashboard за здравето на системите и за издаване на ежедневен обобщаващ отчет, който да позволява на потребителите да открият проблеми, които влияят на цялоста на събраните одитни данни, като лесно да може да се достигне до конкретната детайлна информация, която е необходима, за да се отстранят проблемите. Потребителите да могат да получават email отчет веднъж дневно, който да обобщава извършените действия през последните 24 часа.
REQ.32	Да има централизирана конзола за управление, която да поддържа множество сървъри, като всеки да може да има собствени, различни настройки.
REQ.33	Да позволява интегрирането с други решения, да поддържа одитирането на множество от системи и приложения, включително системи, които са интегрирани чрез RESTful API, като всичко трябва да бъде обединено, позволявайки използването на dashboard-ове и отчети за комплексни среди от разнообразни системи.
REQ.34	Решението да дава цялостен изглед над средата, като всички функционалности да са част от единна платформа, премахвайки необходимостта от използването на множество отделни решения.
REQ.35	Правата за достъп да са ролево базирани. Платформата трябва да позволява фино

	Технически изисквания
	разделяне на задълженията по наблюдението на системите от различните потребители, така че всеки от тях да има достъп само до необходимите му системи и настройки.
REQ.36	Да има напълно документиран RESTful API интерфейс за интеграция с други решения, да може да се интегрира с решения за сигурност, за съответствие с различни сертификати и за автоматизиране на ИТ процесите и на работата на бизнес приложенията, така че да се предостави централизирано одитиране и отчетност или да се улесни управлението на промените и на действията по поддръжката на системите
REQ.37	Да може да се интегрира със SIEM решения, за да се защитят инвестициите на организацията в SIEM платформи, като се предостави интегриране с определени SIEM решения, обогатявайки събраните от тях данни, предоставяйки контекста на събитията
REQ.38	Да позволява безплатно да се добавят add-on добавки за интегриране с други решения, да има възможност за добавяне на безплатни, предварително създадени add-on добавки, които да улесняват интегрирането с решения, като например SIEM, ServiceNow ITSM и Linux системи.
REQ.39	Техническа поддръжка за срок от минимум 5 (пет) години.
REQ.40	Получаване на нови версии на софтуера за срок от минимум 5 (пет) години.
REQ.41	Обновяване на дефиниции и сигнатури за срок от минимум 5 (пет) години.

21. Система за предотвратяване на изтичане на информация извън организацията и загуба на данни от крайните точки (Endpoint DLP)

	Технически изисквания
REQ.1	Предложеното решение трябва да включва функции за DLP мониториране и защита за крайни точки (Endpoint DLP). Цялото решение да бъде предоставено под формата на софтуерен абонамент с включена поддръжка към него. Предложеното решение трябва да включва лицензи за софтуер за 650 потребителя с включени 5 (пет) години поддръжка.
REQ.2	Решението трябва да може да защитава данните на крайните точки (лаптопи, работни станции, сървъри, мобилни устройства).
REQ.3	Решението трябва да може да защитава Windows, Mac OSX и Linux базирани работни станции и сървъри.
REQ.4	Решението трябва да включва специално създадена защита за VDI инфраструктура.
REQ.5	Решението трябва да може минимално да защитава данните на следните приложения: • Outlook, Thunderbird, Apple Mail, Lotus Notes, Evolution; • браузъри IE, Chrome, Firefox, Safari; • SQL, Oracle бази от данни; • източници на данни като Sharepoint, Documentum; • MS Office, Adobe, Libre Office приложения; • в суров програмен код (Visual Studio, Xcode и други); • в CAD системи; • във файлови изображения (jpg, tiff, png, bmp); • в аудио и видео файлове; • в PLM системи (Siemens, Agile и други).
REQ.6	Решението трябва да може да мониторира всички действия с премествания на данни, дори когато няма настроена конкретна политика за това.
REQ.7	Решението трябва да може да отбелязва точните дата и час на действията с премествания на данни.

Технически изисквания	
REQ.8	Решението трябва да може да мониторира и логира всички действия с данни тип Copy, Move, Save As, Open, Close, Read, Write и Edit.
REQ.9	Решението трябва да може да мониторира и логира всички действия за обмен на данни между приложения (cut/copy/paste/printscreen/insert item).
REQ.10	Решението трябва да може да обвързва и отбелязва дадени събития с данни с конкретни потребители, компютърни акаунти и групи от Активната директория.
REQ.11	Решението трябва да може да предоставя инвентарна информация за използваните приложения за обработване на данни.
REQ.12	Решението трябва да може да предоставя информация за йерархията на използваните приложения за обработване на данни (parent и child процеси).
REQ.13	Решението трябва да може да предоставя детайлна информация с пълни характеристики за използваните приложения за обработване на данни (например компания, конкретен продукт, версия, MD5 хеш).
REQ.14	Решението трябва да може да предоставя пълна видимост над всички файлови операции от използвани приложения, включително информация за източника на данните и крайната им дестинация.
REQ.15	Решението трябва да предоставя видимост над операциите с данни, свързани с преносими устройства (например флашки, преносими твърди дискове, Bluetooth устройства).
REQ.16	Решението трябва да може да мониторира и управлява неструктурирани данни като например: • Суров програмен код • Химични формули • Инженерни схеми (CAD) • Файлове, свързани с продуктивност (Office, Adobe, Text файлове) • Файлове с изображения (jpeg, gif, топографии) • Аудио и видео файлове • Криптирани файлове • Архиви
REQ.17	Решението трябва да може да търси в съдържанието на данните, използвайки стрингове, ключови думи, регулярни изрази, съвпадение с термини от речник на решението.
REQ.18	Решението трябва да може да използва „пръстови отпечатъци“ (Fingerprinting) на данни, както и да може да класифицира данните според контекста им.
REQ.19	Решението трябва да може да сканира за данни в покой (At-Rest-Scans)
REQ.20	Решението трябва да може да сканира за данни в движение (On-The-Fly/in motion).
REQ.21	Решението трябва да може да извършва пълно търсене по крайните точки, независимо дали те са онлайн или офлайн.
REQ.22	Решението трябва да може да предоставя функции за събиране на следствена информация за изтичане на данни от тип Key logging (натиснати клавиши от потребителя по време на операцията с данни) по зададени от администратора критерии.
REQ.23	Решението трябва да може да предоставя функции за събиране на следствена информация за изтичане на данни от тип Screen captures (снемане на изображение от дисплея на работната станция по време на операциите с данни) по зададени от администратора критерии.
REQ.24	Събраните следствени данни от решението за изтичане на данни трябва да отговарят на съответните критерии и да са защитени, така че да могат да се използват като доказателство по правни процедури.
REQ.25	Решението трябва да може автоматично да криптира данните при работа с преносими устройства от всякакъв вид.

Технически изисквания	
REQ.26	Решението трябва да може да криптира данните на ниво файл, не само на ниво устройство.
REQ.27	Решението трябва да позволява споделянето на криптирани файлове с трети страни с възможност потребителите да задават пароли за тях.
REQ.28	Решението трябва да позволява криптиране на данни на всякакъв вид преносими твърди носители, като не трябва да е необходимо те да се регистрират като устройства в системата, за да сработи криптирането на тях.
REQ.29	Решението трябва да може да контролира канала за износ на данни чрез преносими устройства на базата на техните характеристики (производител, модел, сериен номер).
REQ.30	Решението трябва да може да контролира канала за износ на данни при работа с приложения, като да може да инспектира буфера на клипборда за класифицирано съдържание при copy/paste операции. Copy/paste операциите да могат да се контролират на базата на локацията на файла източник, съдържанието на файла, класификацията на файла.
REQ.31	Решението трябва да може да контролира printscreen операциите на базата на буферираната информация или на файла източник на екрана.
REQ.32	Решението трябва да може да контролира работата на приложения за улавяне на работата на дисплея (screen capture) от трети страни на базата на буферираната информация или на файла източник на екрана.
REQ.33	Решението трябва да разполага с Advanced Threat Detection функционалност, като агентите на решението трябва да могат да работят в “stealth” режим и да не оставят следи.
REQ.34	Решението трябва да може да предоставя евристични данни от крайните точки (например за поведението на приложения и потребители със засичане на аномално такова).
REQ.35	Решението трябва да предоставя функция за засичане и предотвратяване на заплахи на крайните точки.
REQ.36	Решението и агентите на решението трябва да могат да се интегрират с решения от трети страни за справяне със заплахи (като например PaloAlto, Fidelis, Trellix).
REQ.37	Решението трябва да може да контролира разпространението на зловреден код в средата (malware proliferation).
REQ.38	Решението трябва да предоставя възможност за изграждане на бели/черни списъци от приложения.
REQ.39	Решението трябва да може да оценява рисковите файлове чрез механизъм различен от анализ на файловото разширение, чрез по-детайлни контроли.
REQ.40	Решението трябва да може да използва механизми за засичане на заплахи, за да може да контролира достъпа до класифицирани данни от тях.
REQ.41	Интерфейсът на решението трябва да разполага с DLP и Cyber threat базирани dashboard панели по подразбиране (out of the box).
REQ.42	Интерфейсът на решението трябва да разполага с advanced threat analytics базирани dashboard панели по подразбиране (out of the box).
REQ.43	Интерфейсът на решението трябва да позволява да се филтрира и дълбае в предоставените данни до достигане на конкретна активност за дадено събитие.
REQ.44	Решението трябва да може да се интегрира с Активна директория.
REQ.45	Решението трябва да предоставя отчети със статистически данни за тенденциите на даден потребител, машина, приложение при работа с данни, както и да съдържат информация за нарушени правила от зададените политики.
REQ.46	Решението трябва да предоставя възможност за модифициране на отчетите (customization).
REQ.47	Решението трябва да поддържа ролево-базиран достъп, като да може да се сортира каква

Технически изисквания	
	информация вижда даден потребител или група от потребители според тяхната роля.
REQ.48	Решението трябва да предоставя възможност за анонимизация на данните според дадено потребителско име, име на компютър, път до дестинация на файл.
REQ.49	Решението трябва да може автоматично да изпраща отчети до конкретни потребители или група от потребители. Да се поддържат минимално следните формати: excel, pdf, линк до административната конзола.
REQ.50	Решението трябва да позволява отделните инциденти да се преобразуват в дела за разследване и да могат да се управляват (да могат да се определят кои са отговорните лица по дадено дело и да може да се следят стъпките по него).
REQ.51	Решението трябва да позволява да се извличат данните за събития и вдигнати аларми използвайки Syslog формат.
REQ.52	Решението трябва да позволява извличането на данни за целите на предоставяне на SIEM решения от трети страни, като извлечените данни да могат да са в подходящи за тях формати, минимално Arcsight CEF, Qradar LEEF, Splunk CIM.
REQ.53	Решението трябва да може да предоставя известия на базата на дадена политика или правило.
REQ.54	Решението трябва да може да вдига аларми за инциденти, като те да могат да се изпращат в реално време по email до зададени лица.
REQ.55	Решението трябва да позволява key logging функцията да може да бъде конфигурирана за конкретни крайни точки или потребители на базата на политика.)
REQ.56	Решението трябва да може да улавя дисплея на крайните точки (screen capture) като функцията да може да бъде конфигурирана на базата на политика.
REQ.57	Решението трябва да предоставя функция за заглушени аларми (Silent Alert).
REQ.58	Решението трябва да може да изпраща известия до замесените потребители по зададена политика.
REQ.59	Решението трябва да може да изпрати запитване за причина за дадено действие (justification) до замесените потребители по зададена политика.
REQ.60	Решението трябва да може да блокира действия с данни по зададена политика.
REQ.61	Решението трябва да постави дадена крайна точка под карантина по зададена политика.
REQ.62	Решението трябва да предоставя възможност на администраторите да поискат извличането на замесен файл по зададена политика.
REQ.63	Решението трябва да разполага с Process vaulting функция (да може да маркира даден процес като чувствителен на базата на конкретни характеристики).
REQ.64	Решението трябва да поддържа използването на променливи броячи за изграждането на правилата на политиките.
REQ.65	Агентите на решението трябва да могат да се поставят чрез използването на стандартни инструменти за разпространение на софтуер.
REQ.66	Решението трябва да поддържа "тих" тип инсталация на агенти.
REQ.67	Решението трябва да поддържа LDAP интеграция.
REQ.68	Решението трябва да поддържа използването на криптирана връзка тип клиент-сървър и обратно за управление на решението.
REQ.69	Решението трябва да разполага с графичен интерфейс за управление, достъпен чрез уеб-браузър, като от него да могат да се извършват всички действия за изграждане на политики и изготвяне на отчети.
REQ.70	Агентите на решението да имат минимално отражение върху производителността на крайните точки.
REQ.71	Функцията на агентите за инспектиране на съдържанието на данните да има минимално отражение върху производителността на крайните точки.

Технически изисквания	
REQ.72	Базовите функции на агентите да не изискват постоянен мрежови достъп до сървърните компоненти на решението за изпълнението им, включително операциите за инспектиране на съдържанието на данните.
REQ.73	Софтуерна поддръжка от производителя: 5 години
REQ.74	Тип поддръжка: 24x7x365
REQ.75	Възможност за обновление на софтуера в периода на поддръжката

III. Параметри на оборудването

Оборудването (хардуер и софтуер), предмет на доставката, трябва да бъде фабрично ново, неупотребявано, да е в актуалните продуктови листи на производителя и да не е спряно от производство.

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.

Хардуерът следва да бъде доставен в пълно работно състояние, в оригиналната опаковка на производителя с не нарушена цялост, окомплектовано с всички необходими интерфейсни и захранващи кабели, където се изискват, както и с необходимата техническа документация (на хартиен или електронен носител).

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

IV. Изисквания към изпълнението

Изпълнителят осигурява онлайн система за управление на заявки (СУЗ) за регистриране и проследяване на статуса на изпълнението им. Всички получени заявки по телефон следва да бъдат вписани и в СУЗ.

В СУЗ се вписват заявки, свързани с гаранционното обслужване на доставените устройства, както и рекламации.

V. Място на изпълнение

Мястото на извършване на доставката е АГКК, ул. „Мусала“ № 1