Приложение № 2
към рамков договор № ПО-16-3528/21.12.2023 г.

ЗАЯВКА по Рамков договор № ПО-16-3528 от 21.12.2023 г.		☑
ЗАЯВКА по Рамков договор № ПО-16-3528 от 21.12.2023 г. (актуализирана)		☐[1]
Позиция от ПГ-2025 г.:	*№ по ред от ПГ* ***8***	Осигуряване на отказоустойчива, резервирана, производителна, защитена и документирана информационна и комуникационна инфраструктура (ИКИ) на НАП
Описание на проект съгласно ПГ:	Осигуряване на отказоустойчива, резервирана, производителна, защитена и документирана информационна и комуникационна инфраструктура (ИКИ) на НАП.	
CPV код	48517000-5 Софтуерни пакети за информационни технологии 30236000-2 Различни видове компютърен хардуер 72611000-6 Услуги по оказване на техническа помощ в областта на компютърните системи	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	МЕУ-9929/09.07.2025 г.	
Изискване за достъп до класифицирана информация ДА/НЕ	НЕ	
Стойност: (*стойността следва да съответства на заложената в План-графика***) без ДДС***, в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово*		40 744 540,00 [2] лв. Дейност 1: 9 250 000,00 лв. Дейност 2: 7 924 980,00 лв. Дейност 3: 5 731 630,00 лв. Дейност 4: 17 837 930,00 лв.
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*		На части след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на всяка извършена доставка/услуга по съответната дейност
Плащане с акредитив или авансово ДА/НЕ		НЕ
Документи за плащане с акредитив или авансово		НЕ

[1] Отбелязва се в случай че заявката е актуализирана
[2] Заявката е без осигурено финансиране към 09.07.2025 г. и подлежи на изпълнение след писмено уведомление за осигурено финансиране от страна на Бенефициера до Изпълнителя

Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	Срок за осигуряване: до 6 месеца от подписване на заявката Валидност: съгласно ТП	
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	Съгласно ТП	
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*	На части след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на всяка извършена доставка/услуга по съответната дейност	
Приложения: (*напр: технически параметри, образци на отчетни документи***)**	Технически параметри (ТП)	
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		
ЗАЯВКАТА е ИЗГОТВЕНА ОТ:		
Ръководител на проект по заявката от страна на БЕНЕФИЦИЕРА (напр: представител на дирекцията – Заявител):		
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Координатор на договора от страна на ВЪЗЛОЖИТЕЛЯ:		

Ръководител на договора от страна на БЕНЕФИЦИЕРА:		
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Ръководител на проект по заявката		
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		

Забележка: *С една заявка могат да се възлагат повече от един проект по ПГ, само когато те са еднотипни и управлението им (възлагане, изпълнение, отчитане) може да се извършва съгласно описаните в таблицата от заглавната страница на заявката параметри и лица. В този случай в таблицата се добавят необходимия брой редове, за описване на съответните проекти. Когато проектите не са еднотипни, те се възлагат с отделни заявки.*

Приложение 1

ТЕХНИЧЕСКИ ПАРАМЕТРИ
ПО ПРОЕКТ
„Осигуряване на отказоустойчива, резервирана, производителна, защитена и документирана информационна и комуникационна инфраструктура (ИКИ) на НАП“

Гр. София, 2025 г.

I. Въведение. Цел на документа.

Национална агенция за приходите (НАП) разполага с цялостна информационна и комуникационна инфраструктура (ИКИ) и решения за кибер защита, изградена по модела defense in depth. Това е комплексен подход, осигуряващ защита в различни нива. По-голямата част от компонентите на тази ИКИ са доставени през 2020 г. и 2022 г., въз основа на проведени открити процедури по реда на Закона за обществените поръчки (ЗОП). През 2025 г. е необходимо подновяване на хардуерната поддръжка на устройствата, както и на лицензите, асоциирани с тяхната функционалност.

Освен това е планирано надграждане и оптимизиране на ИКИ на НАП чрез доставката на ново допълнително оборудване и софтуер, с оглед необходимостта от гарантиране на устойчивост, сигурност, оперативна съвместимост и ефективност на системите на приходната агенция.

Въз основа на гореописаната фактическа обстановка е констатирана необходимостта от реализиране на проект с предмет: „Осигуряване на отказоустойчива, резервирана, производителна, защитена и документирана информационна и комуникационна инфраструктура (ИКИ) на НАП“ (проекта).

Изпълнението на проекта е организирано в 4 основни дейности, както следва:

1. **Дейност 1 „Осигуряване на хардуерна и софтуерна поддръжка на налична комуникационна техника и доставка на ново допълнително комуникационно оборудване“**;
2. **Дейност 2: „Осигуряване на решение за виртуализация, хардуерна и софтуерна поддръжка на оборудване и доставка на ново допълнително прилежащо оборудване**“.
3. **Дейност 3: „Осигуряване и поддръжка на решения за одит и анализ на промените, решение за управление на привилегирования достъп до отдалечени ресурси (Privileged Access Management - PAM), решение за предотвратяване на загуба на данни и решение за защита и управление на уязвимости, софтуерни лицензи на система за събиране и анализ на логове, осигуряване на хардуерна поддръжка и продължаване правото на ползване и поддръжка за устройства и софтуерни лицензи за защита на Web приложения, осигуряване на нови защитни стени втори слой“;**
4. **Дейност 4: „Осигуряване на решение за защита на крайни потребители, e-mail среда, мрежова инфраструктура“.**

Настоящият документ има за цел да опише минималните изисквания към подновяването на хардуерната и софтурната поддръжка на внедрените в НАП решения, както и доставката на ново допълнително оборудване и софтуерни продукти.

II. Дейност 1: „Осигуряване на хардуерна и софтуерна поддръжка на налична комуникационна техника и доставка на ново допълнително комуникационно оборудване“

1. Поддейност 1.1. Осигуряване на хардуерна и софтуерна поддръжка на наличната комуникационна техника, подробно описана в Таблица № 1 и Таблица № 2:

В обхвата на тази поддейност изпълнителят трябва да осигури хардуерна и софтуерна поддръжка на наличната комуникационна техника съгласно Таблица № 1 иТаблица № 2 по-долу.

А) Осигуряване на хардуерна и софтуерна поддръжка съгласно описаното в Таблица 1

Таблица № 1

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
REQ.1.	ISR4451-DNA	36	FGL2438L492 FGL2438L3EL FGL2438L2WY FGL2438L31N FGL2438L4RY FGL2438L48X FGL2438L2XE FGL2438L2YT FGL2438L35X FGL2438L33U FGL2438L3L6 FGL2438L31G FGL2438L3F8 FGL2438L49E FGL2438L36W FGL2438L3KB FGL2438L3DQ FGL2438L2ZV FGL2438L3ET FGL2438L32K FGL2438L3L3 FGL2438L4Y1 FGL2438L49S FGL2438L315 FGL2438L354 FGL2438L3E8 FGL2438L2WQ FGL2438L3LX	06.11.2025	30.11.2028

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FGL2438L34E FGL2438L339 FGL2438L3GB FGL2438L342 FGL2438L364 FGL2438L3LK FGL2438L376 FGL2117820S		
REQ.2.	ISR1100-6G	42	FGL2441L6JA FGL2441L780 FGL2441L37Z FGL2441L37N FGL2441L77Z FGL2441L77X FGL2441L77U FGL2441L77R FGL2441L77P FGL2441L77N FGL2441L77M FGL2441L77L FGL2441L77H FGL2441L77F FGL2441L77D FGL2441L77B FGL2441L779 FGL2441L778 FGL2441L6JL FGL2441L6JK FGL2441L6JH FGL2441L6JG FGL2441L6JF FGL2441L6JD FGL2441L6JB FGL2441L790 FGL2441L78T FGL2441L78S FGL2441L78R FGL2441L78Q FGL2441L78P FGL2441L78N FGL2441L78M FGL2441L78L FGL2441L78H	06.11.2025	31.12.2028

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FGL2441L78F FGL2441L78E FGL2441L78A FGL2441L788 FGL2441L784 FGL2441L781 FGL2441L382		
REQ.3.	ISR1100-4G	36	FGL2441L6KP FGL2441L6LE FGL2441L6KM FGL2441L6KL FGL2441L6KJ FGL2441L6KH FGL2441L6KG FGL2441L6KF FGL2441L6KE FGL2441L6KC FGL2441L6KB FGL2441L6KA FGL2441L6K7 FGL2441L6LC FGL2441L6LB FGL2441L6LA FGL2441L6L9 FGL2441L6L8 FGL2441L6L7 FGL2441L6L6 FGL2441L6L5 FGL2441L6L4 FGL2441L6L3 FGL2441L6L2 FGL2441L6L0 FGL2441L6KZ FGL2441L6KY FGL2441L6KX FGL2441L6KW FGL2441L6KV FGL2441L6KU FGL2441L6KT FGL2441L6KR FGL2441L6KQ FGL2441L6LF FGL2441L6KN	06.11.2025	31.12.2028

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
REQ.4.	C9300-24P-A	32	FOC2433L40X FOC2433L428 FOC2433L5DC FOC2433L5CY FOC2433L5BY FOC2433L42B FOC2433L5BD FOC2433L5CW FOC2433L56P FOC2433L5CX FOC2433L5BV FOC2432LBVQ FOC2433L5FH FOC2433L5CV FOC2433L42K FOC2433L409 FOC2433L3Q4 FOC2433L43D FOC2433L5DL FOC2433L3X7 FOC2433L5DX FOC2433L5B4 FOC2433L3N6 FOC2433L5C4 FOC2433L56X FOC2432L94M FOC2433L5F2 FOC2433L3ZZ FOC2433L56Y FOC2433L5AR FOC2433L5AS FOC2433L5CF	06.11.2025	31.12.2028
REQ.5.	C9300-24S-A	2	FOC2433L8XP FOC2433L8Y8	06.11.2025	31.12.2028
REQ.6.	C9300-48T-A	7	FOC2431L277 FOC2431L27A FOC2431L22X FOC2431L2L4 FOC2431L26B FOC2431L27U FOC2431L275	06.11.2025	31.12.2028
REQ.7.	C9606R	4	FXS2438Q1DQ	06.11.2025	31.12.2028

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FXS2439Q00X FXS2439Q00V FXS2439Q01B		
REQ.8.	C9200L-48T-4G-E	14	JAE234802XL JAE234803HF JAE23480389 JAE234803A9 JAE234803N0 JAE234802XK JAE2348030L JAE234803MF JAE234803DV JAE234803GX JAE234803FG JAE234803LX JAE23480364 JAE234803AN	31.12.2026	31.12.2028
REQ.9.	ASR1001-HX	2	TTM242802SJ TTM2429005V	06.11.2025	31.12.2028
REQ.10.	DN2-HW-APL	3	WMP242900MG WMP242900M8 WMP242900LX	06.11.2025	31.12.2028
REQ.11.	C9300-24P-A	431	FOC2639YB41 FOC2639YB69 FOC2640Y5F8 FOC2640Y5CL FOC2640Y5EU FOC2639YB6B FOC2641Y642 FOC2641Y5G9 FOC2641Y5HH FOC2641Y5HK FOC2641Y5JD FOC2641Y5JT FOC2641Y5KD FOC2641Y5N2 FOC2641Y5NU FOC2641Y5P1 FOC2641Y5PJ FOC2641Y5PM FOC2641Y5Q3 FOC2641Y5Q9 FOC2641Y5S9	20.11.2027	31.12.2028

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FOC2641Y5YQ FOC2641Y5Z1 FOC2641Y5ZF FOC2641Y5ZQ FOC2639YRAN FOC2640Y1L5 FOC2640Y6EX FOC2640Y6F0 FOC2640Y6F1 FOC2640Y6GL FOC2640Y81D FOC2640Y81F FOC2640Y81U FOC2641Y4ZE FOC2641Y51F FOC2641Y520 FOC2641Y528 FOC2641Y52M FOC2641Y5DR FOC2641Y5E3 FOC2641Y5F0 FOC2641Y5G8 FJC26251D7M FJC26251D8Z FJC26251D9J FJC26251DAA FJC26261NYZ FOC2622Y0BK FOC2622Y0BY FOC2630YAB0 FOC2632YH6R FOC2634YHZ3 FOC2634YM3T FOC2637YAG2 FOC2637YDJH FOC2637YH8L FOC2639Y6B3 FOC2639Y6BJ FOC2639Y6FS FOC2639YLKZ FJC26251D3Y FJC26251D4C FJC26251D60		

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FJC26251C5E FJC26251C7S FJC26251D7B FJC26251D7D FJC26251C82 FJC26251C8U FJC26251CLM FJC26251CQR FJC26251CRH FJC26251CU8 FJC26251D10 FJC26251D1C FJC26251D1Y FJC26251D28 FJC26251D29 FOC2641Y9V5 FOC2641Y9W6 FOC2641Y9WB FOC2641Y9WD FOC2641Y9WW FOC2641Y9X3 FOC2641Y9X6 FOC2641Y9XF FOC2641Y9XG FOC2641Y9XP FOC2641Y8Z0 FOC2641Y8Z3 FOC2641Y8ZQ FOC2641Y8ZY FOC2641Y90M FOC2641Y91H FOC2641Y91J FOC2641Y91P FOC2641Y91Q FOC2641Y92N FOC2641Y92P FOC2641Y931 FOC2641Y939 FOC2641Y93G FOC2641Y97N FOC2641Y97S FOC2641Y982 FOC2641Y9AQ		

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FOC2641Y8TK FOC2641Y8UB FOC2641Y8VV FOC2641Y8WW FOC2641Y8X3 FOC2641Y8XB FOC2641Y8XN FOC2641Y8XR FOC2641Y8XX FOC2641Y8Y1 FOC2641Y8Y5 FOC2641Y8YE FOC2641Y8YF FOC2641Y8YY FOC2641Y4ZP FOC2641Y826 FOC2641Y8NM FOC2641Y8TH FOC2641YA6B FOC2641Y9XT FOC2641Y9XV FOC2641Y9YK FOC2641Y9ZW FOC2641YA0B FOC2641YA0L FOC2641YA0V FOC2641YA10 FOC2641YA12 FOC2641YA1A FOC2641YA1E FOC2641YA1J FOC2641YA2K FOC2641YA2X FOC2641YA37 FOC2641YA3F FOC2641YA3Q FOC2641YA4U FOC2641Y9P3 FOC2641Y9QL FOC2641Y9QS FOC2641Y9RH FOC2641Y9SF FOC2641Y9SL		

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FOC2641Y9SR FOC2641Y9TC FJC26251J55 FJC26251J5A FOC2622Y0B6 FOC2622Y0BU FOC2622Y341 FOC2622Y3PR FOC2622Y3R6 FOC2622Y3T0 FOC2622Y3T3 FOC2622Y3TG FOC2622Y3U4 FOC2622Y3X0 FOC2641Y5F2 FOC2641Y5FW FJC26251J26 FJC26251J2K FJC26251J2P FJC26251J2R FJC26251J32 FJC26251J33 FJC26251J35 FJC26251J36 FJC26251J38 FJC26251J39 FJC26251J3B FJC26251J3D FJC26251J3F FJC26251J3H FJC26251J3K FJC26251J3L FJC26251J3N FJC26251J3V FJC26251D9X FJC26251DAS FJC26251DE3 FJC26251FFQ FJC26251H2F FJC26251H89 FJC26251HBT FJC26251HC5 FJC26251HQR		

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FJC26251HRH FJC26251HXD FJC26251HXZ FJC26251HY0 FJC26251J0C FJC26251J1L FJC26251J1Q FJC26251J1W FJC26251J24 FJC26251D2J FJC26251D2S FJC26251D3W FJC26251C52 FJC26251C77 FJC26251CB9 FJC26251CFJ FJC26251CL4 FJC26251CQD FJC26251CQP FJC26251CS3 FJC26251CU5 FJC26251D5B FJC26251D98 FJC26251CUP FJC26251D0S FJC26251D0T FJC26251D0V FOC2641Y5N0 FJC26251J49 FJC26251J4A FJC26251J4K FJC26251J4V FJC26271M4R FJC26261H6R FJC26261H6X FJC26261H6Y FJC26261H77 FJC26261H7E FJC26261H7N FJC26261H8A FJC26261H92 FJC26261H9Q FJC26261HA5		

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FJC26261HD6 FJC26261HE9 FJC26261HF0 FJC26261HF1 FJC26261HFL FJC26261HGU FJC26261HJK FJC26261HNE FJC26261GRR FJC26261GT3 FJC26261GU9 FJC26261GVD FJC26261GWH FJC26261GZM FJC26261H05 FJC26261H0S FJC26261H2K FJC26261H2S FJC26261H49 FJC26261H4U FJC26261H4W FJC26261H4Z FJC26261H55 FJC26261H57 FJC26261H62 FJC26261H6J FJC26251DAM FJC26251DAQ FJC26251DCV FJC26251DCX FJC26251DL5 FJC26251DLP FJC26251DN5 FJC26251J1U FJC26251J2Q FJC26261176 FJC26261GEQ FJC26261GGL FJC26261GKX FJC26261GN3 FJC26261GNC FJC26261GNW FJC26261GPT		

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FJC26261GQY FJC26251D7G FJC26251D8G FJC26251D96 FJC26251D9C FJC262512US FJC262515WQ FJC262515XE FJC262515Y2 FJC262516KK FJC26251CBT FJC26251CE8 FJC26251CFQ FJC26251CRG FJC26251CTQ FJC26251D00 FJC26251D37 FJC26251D6F FJC26251D7A FOC2641YA74 FOC2641Y9YF FOC2641Y9YQ FOC2641Y9YX FOC2641Y9ZX FOC2641YA01 FOC2641YA19 FOC2641YA20 FOC2641YA2L FOC2641YA31 FOC2641YA3G FOC2641YA3L FOC2641YA4V FOC2641YA54 FOC2641YA5E FOC2641YA6C FOC2641YA6J FOC2641YA70 FOC2641Y9RK FOC2641Y9RS FOC2641Y9RW FOC2641Y9S6 FOC2641Y9SA FOC2641Y9SP		

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FOC2641Y9UB FOC2641Y9UJ FOC2641Y9UM FOC2641Y9V6 FOC2641Y9V8 FOC2641Y9VE FOC2641Y9VU FOC2641Y9WG FOC2641Y9WS FOC2641Y9XN FOC2641Y9XX FOC2641Y9Y4 FOC2622Y3VU FOC2622Y3YM FOC2622Y3ZD FOC2622Y3ZE FOC2622Y40C FOC2622Y40P FOC2622Y45X FOC2622Y468 FOC2641Y8R0 FOC2641Y95Z FOC2641Y9P9 FOC2641Y9PE FOC2641Y9PY FOC2641Y9Q4 FOC2641Y9QT FOC2641Y9R7 FOC2641Y9RB FOC2641Y9RG FOC2622Y3PL FOC2622Y3PN FJC26251CBM FJC26251D73 FJC26251D8B FJC26251HCC FJC26251HD3 FJC26251HN6 FJC26251HRD FJC26251HRJ FOC2622Y3PP FOC2622Y3RS FJC26251HTR		

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FJC26251J0H FJC26251J37 FJC26251J3R FOC2622Y3LP FOC2622Y3MU FOC2641YADW FOC2641YADU FOC2641YALB FOC2641Y9C4 FOC2641Y9EG FOC2641Y9EL FOC2641Y9UW FOC2641Y9VA FOC2641Y9VH FOC2641Y9Y0 FOC2641Y9ZY FOC2641YA02 FOC2641Y5EU FOC2641Y5FP FOC2641Y5GN FOC2641Y5R4 FOC2641Y5ZV FOC2641Y60F FOC2641Y60J FOC2641Y633 FOC2641YA1K FOC2641YANM FOC2641YANV FOC2641YAPD FOC2641YAPJ FOC2641YAPN FOC2641YAPU FOC2641YALM FOC2641YALN FOC2641YALQ FOC2641YALW FOC2641YALX FOC2641YALY FOC2641YAM6 FOC2641YAM7 FOC2641YAM8 FOC2641YAMD FOC2641YAMG		

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FOC2641YAMK FOC2641YAMS FOC2641YAMU FOC2641YAN3 FOC2641YAN4 FOC2641YANE FOC2641YANF FOC2641YA1T FOC2641YA1X FOC2641YA21 FOC2641YA3S FOC2641YA5D FOC2641YA82 FOC2641YA8L FOC2641YA8P FOC2641YA91 FOC2641YA9D FOC2641YAAD FOC2641YAAS FOC2641YAAW FOC2641YADD FOC2641YAL7 FVH2737L28Y		
REQ.12.	C9300-24T-A	42	FOC2642YB6J FOC2642YC3X FOC2642YB7K FOC2642YBKR FOC2642YBKV FOC2642YBP0 FOC2642YBPZ FOC2642YBQW FOC2642YBQY FOC2642YBRG FOC2642YBTG FOC2642YBTL FOC2642YBUW FOC2642YBZP FOC2642YC1L FOC2642YC26 FOC2642YC2B FOC2642YC3A FOC2642YA9E	20.11.2027	31.12.2028

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FOC2642YADC FOC2642YAPB FOC2642YAQU FOC2642YAR9 FOC2642YARU FOC2642YASP FOC2642YASV FOC2642YATF FOC2642YAUU FOC2642YAUV FOC2642YAVL FOC2642YAZ5 FOC2642YB0X FOC2642YB3V FOC2642Y9NL FOC2642YB4W FOC2642YB64 FOC2642YC3G FOC2642YC3H FOC2642YC3W FOC2642YB6Y FOC2642YBUB FOC2642YACD		
REQ.13.	C9300-24S-A	2	FOC2624YCGA FOC2624YCGL	29.09.2027	31.12.2028
REQ.14.	C9300X-24Y-A	40	FOC2621Y27V FOC2622Y0K7 FOC2621Y1VF FOC2620Y7CF FOC2618YPPE FOC2618YP4D FOC2618YHZ9 FOC2618YH8L FOC2617Z1UV FOC2617YXUD FOC2617YTL6 FOC2617YTFP FOC2617YE7M FOC2617YD61 FOC2548Y86P FOC2548Y2W5 FOC2544YPNL	29.09.2027	31.12.2028

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FOC2536YBFT FOC2622Y0K5 FOC2622Y0K1 FOC2622Y0K0 FOC2622Y0J7 FOC2621Y4HP FOC2621Y4CA FOC2621Y3QK FOC2621Y3NP FOC2621Y3NN FOC2621Y3NF FOC2621Y3ND FOC2621Y3NC FOC2621Y3NB FOC2621Y2WD FOC2621Y28Q FOC2621Y289 FOC2621Y285 FOC2621Y27Z FOC2622Y0N0 FOC2622Y0MX FOC2622Y0M7 FOC2621Y1VY		
REQ.15.	WS-C3560CX-12PC-S	47	FOC2022W0NV FOC2646YASW FOC2646YA4E FOC2646YATE FOC2646YAUH FOC2646YAUK FOC2646YAW1 FOC2646YAW2 FOC2646YAWB FOC2646YAWD FOC2646YAWE FOC2646YAWJ FOC2646YA4P FOC2646YA4Q FOC2646YA53 FOC2646YA58 FOC2646YA5C FOC2646YA5H FOC2646YA63 FOC2646YA67	08.12.2027	31.12.2028

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FOC2646YA69 FOC2646YA6A FOC2646YA88 FOC2646YA8B FOC2646YA8G FOC2646YADA FOC2646YAJ2 FOC2646YAQV FOC2646YARF FOC2646YAS0 FOC2645YCZG FOC2645YCZJ FOC2646Y0XE FOC2646Y0Y8 FOC2646Y0Y9 FOC2646YA24 FOC2646YA26 FOC2646YA27 FOC2646YA2S FOC2646YA31 FOC2646YA3R FOC2646YA3S FOC2645YCY9 FOC2645YCZ7 FOC2646YAT2 FOC2736Y54X FOC2749Y2SV		
REQ.16.	C9300-24P-A	69	FVH2813L872 FVH2813L87A FVH2813L87B FVH2813L87C FVH2813L3B9 FVH2813L3BC FVH2813L3ZS FVH2813L3ZV FVH2813L44R FVH2813L564 FVH2813L82N FVH2813L82X FVH2813L82Z FVH2813L833 FVH2813L836 FVH2813L83A	11.06.2027	31.12.2028

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FVH2813L83D FVH2813L83E FVH2813L83H FVH2813L83Z FVH2813L85S FVH2810L47E FVH2810L48R FVH2810L490 FVH2810L496 FVH2810L4A8 FVH2810L4BA FVH2810L4BD FVH2810L4BR FVH2812L00B FVH2812L577 FVH2812L595 FVH2812L774 FVH2812L7YJ FVH2813L1D1 FVH2813L1D9 FVH2813L343 FVH2813L34V FVH2810L41Y FVH2810L436 FVH2810L43C FVH2810L43U FVH2810L44Q FVH2810L45D FVH2810L45T FVH2810L45W FVH2810L46K FVH2810L46U FVH2810L3DS FVH2810L3TK FVH2810L3US FVH2810L405 FVH2810L417 FVH2810L418 FVH2810L47B FVH2813L897 FVH2813L85V FVH2813L85X FVH2813L85Y		

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
			FVH2813L85Z FVH2813L865 FVH2813L866 FVH2813L867 FVH2813L86A FVH2813L86D FVH2813L86L FVH2813L86Y FVH2813L86Z FVH2813L871		
REQ.17.	C9200L-24T-4G-E	8	FVH28020BM3 FVH28020BMM FVH28020BN2 FVH28020BTN FVH28020BRZ FVH28020BSJ FVH28020BTE FVH28020BQU	11.06.2027	31.12.2028
REQ.18.	C9200L-48T-4G-E	8	FVH28071PCM FVH28071PFR FVH28071PTQ FVH28071PBW FVH28071Q25 FVH28071Q4W FVH28071P83 FVH28071Q0X	11.06.2027	31.12.2028
REQ.19.	C9200CX-12P-2X2G-E	3	FJC28091CSH FJC28091CW4 FJC28091E5V	11.06.2027	31.12.2028
REQ.20.	N9K-C9332C	2	FDO24341CUZ FDO24341CW3	06.11.2025	31.12.2028
REQ.21.	APIC-CLUSTER-M3	1	Номер на сервизния идентификатор - 5500912185	06.11.2025	31.10.2028
REQ.22.	N9K-C93180YC-FX-B. Комутаторите са част от бъндел N9K-C93180-FX-B24C	2	FDO24081JG1 FDO243006Y2	06.11.2025	31.12.2028
REQ.23.	FPR4115-NGFW-K9	2	JMX2441L02A JMX2441L02B	06.11.2025	31.12.2028

№	Вид или продуктов номер	Брой	Серийни номера	Период на текуща валидност до:	Период на валидност до:
REQ.24.	FPR4K-NM-4X40G	2	JAD24360UEW JAD24360UFE	06.11.2025	31.12.2028
REQ.25.	ST-SMC2210-K9	1	WZP26400140	17.10.2027	31.10.2028
REQ.26.	ST-FC4210-K9	1	WZP2640013Q	17.10.2027	31.10.2028
REQ.27.	TG-M5-K9	1	WZP26100L2Y	11.07.2027	31.10.2028
REQ.28.	C9606R	4	FXS2438Q1DQ FXS2439Q00X FXS2439Q00V FXS2439Q01B	06.11.2025	31.12.2028

Б) Осигуряване на лицензи за продължаване на правото на ползване и поддръжка, съгласно Таблица 2:

Таблица № 2

№	Вид или продуктов номер	Описание	Брой	Период на текуща валидност до:	Период на валидност до:
REQ.1.	SDWAN лиценз Advantage Tier 3	EA SDWAN Advantage Tier 3 лиценз. Номер на договора за правото на ползване и поддръжка-Sub673538	2	06.11.2025	31.12.2028
REQ.2.	SDWAN лиценз Advantage Tier 2	EA SDWAN Advantage Tier 2 лиценз Номер на договора за правото на ползване и поддръжка - Sub673538	78	06.11.2025	31.12.2028
REQ.3.	SDWAN лиценз Advantage Tier 1	EA SDWAN Advantage Tier 1 лиценз Номер на договора за правото на ползване и поддръжка - Sub673538	36	06.11.2025	31.12.2028
REQ.4.	LiveNX лиценз	LiveNX лиценз за устройство. Номер на лиценза a0f2G00000I5rpz	116	06.11.2025	31.12.2028

№	Вид или продуктов номер	Описание	Брой	Период на текуща валидност до:	Период на валидност до:
REQ.5.	DNA лиценз за C9300 24	DNA лиценз за Cisco C9300-24P-A. Номер на договора за правото на ползване и поддръжка - 203512949	32	06.11.2025	31.12.2028
REQ.6.	DNA лиценз за C9300 24S	DNA лиценз за Cisco C9300-24S-A. Номер на договора за правото на ползване и поддръжка - 203512949	2	06.11.2025	31.12.2028
REQ.7.	DNA лиценз за C9300 48	DNA лиценз за Cisco C9300-48T-A. Номер на договора за правото на ползване и поддръжка - 203512949	7	06.11.2025	31.12.2028
REQ.8.	DNA лиценз за C9600	DNA лиценз за Cisco C9606R. Номер на договора за правото на ползване и поддръжка - 203512949	2	06.11.2025	31.12.2028
REQ.9.	DNA лиценз за C9600	DNA лиценз за Cisco C9606R. Номер на договора за правото на ползване и поддръжка - 203512949	2	06.11.2025	31.12.2028
REQ.10.	C9200L-DNA-E-48=	DNA Essentials лиценз за Cisco C9200L-48T-4G-E. Номер на договора за правото на ползване и поддръжка - 206114257	14	31.12.2026	31.12.2028
REQ.11.	SLASR1-AES	AES лиценз за рутер Cisco ASR1001-HX. Номер на договора за правото на ползване и поддръжка - 203861822	2	06.11.2025	31.12.2028

№	Вид или продуктов номер	Описание	Брой	Период на текуща валидност до:	Период на валидност до:
REQ.12.	FLSASR1-AVC	AVC лиценз за рутер Cisco ASR1001-HX. Номер на договора за правото на ползване и поддръжка - 203861822	2	06.11.2025	31.12.2028
REQ.13.	FLSASR1-IOSRED	IOS Redundancy лиценз за рутер Cisco ASR1001-HX. Номер на договора за правото на ползване и поддръжка - 203861822	2	06.11.2025	31.12.2028
REQ.14.	C9300-DNA-A-24=	DNA Advantage лиценз за Cisco C9300-24P-A. Номер на договора за правото на ползване и поддръжка - 205088428	473	20.11.2027	31.12.2028
REQ.15.	C9300-DNA-A-24S=	DNA Advantage лиценз за Cisco C9300-24S-A. Номер на договора за правото на ползване и поддръжка - 205088428	2	29.09.2027	31.12.2028
REQ.16.	C9300X-DNA-24Y-A=	DNA Advantage лиценз за Cisco C9300X-24Y-A. Номер на договора за правото на ползване и поддръжка - 205088428	40	29.09.2027	31.12.2028
REQ.17.	C3560CX-DNA-A-12=	DNA Advantage лиценз за Cisco WS-C3560CX-12PC-S. Номер на договора за правото на ползване и поддръжка - 205088428	47	08.12.2027	31.12.2028
REQ.18.	C9300-DNA-A-24=	DNA Advantage лиценз за Cisco	69	11.06.2027	31.12.2028

№	Вид или продуктов номер	Описание	Брой	Период на текуща валидност до:	Период на валидност до:
		C9300-24P-A. Номер на договора за правото на ползване и поддръжка - 206072466			
REQ.19.	C9200L-DNA-E-24=	DNA Essentials лиценз за Cisco C9200L-24T-4G-E. Номер на договора за правото на ползване и поддръжка - 206072466	8	11.06.2027	31.12.2028
REQ.20.	C9200L-DNA-E-48=	DNA Essentials лиценз за Cisco C9200L-48T-4G-E. Номер на договора за правото на ползване и поддръжка - 206072466	8	11.06.2027	31.12.2028
REQ.21.	C9200CX-DNA-E-12=	DNA Essentials лиценз за Cisco C9200CX-12P-2X2G-E. Номер на договора за правото на ползване и поддръжка - 206072466	3	11.06.2027	31.12.2028
REQ.22.	ACI-SEC-XF	Софтуерен лиценз за комутатор N9K-C9332C. Номер на договора за правото на ползване и поддръжка - 203861822	2	06.11.2025	31.12.2028
REQ.23.	ACI-SEC-XF=	Софтуерен лиценз за комутатор N9K-C93180YC-FX-B. Номер на договора за правото на ползване и поддръжка - 203861822	2	06.11.2025	31.12.2028
REQ.24.	Лиценз за комутатор N9K-	Софтуерен лиценз DCN Premier за	2	06.11.2025	31.12.2028

№	Вид или продуктов номер	Описание	Брой	Период на текуща валидност до:	Период на валидност до:
	C93180YC-FX-B	комутатор N9K-C93180YC-FX-B. Номер на договора за правото на ползване и поддръжка - Sub651607			
REQ.25.	ISE-A-LIC	Advantage лиценз за Cisco Identify Service Engine. Номер на договора за правото на ползване и поддръжка - Sub1362138	11000	08.12.2027	31.12.2028
REQ.26.	Лиценз за Cisco Email Security	Потребителски лиценз за Cisco Email Security. Номер на договора за правото на ползване и поддръжка - Sub876190	8300	06.11.2025	31.12.2028
REQ.27.	SMA-EMGT-LIC	Лиценз за централно управление на Cisco Email Security. Номер на договора за правото на ползване и поддръжка - Sub876190	8300	06.11.2025	31.12.2028
REQ.28.	WSA-WSE-LIC	Потребителски лиценз Essentials за Cisco Web Security. Номер на договора за правото на ползване и поддръжка - Sub876189	8300	06.11.2025	31.12.2028
REQ.29.	WSA-AMP-LIC	Потребителски лиценз за използване на Advanced Malware Protection в Cisco Web Security. Номер на договора за правото на ползване и поддръжка - Sub876189	8300	06.11.2025	31.12.2028

№	Вид или продуктов номер	Описание	Брой	Период на текуща валидност до:	Период на валидност до:
REQ.30.	SMA-WMGT-LIC	Лиценз за централно управление на Cisco Web Security. Номер на договора за правото на ползване и поддръжка - Sub876189	8300	06.11.2025	31.12.2028
REQ.31.	L-FPR4115T-TM=	Лиценз за използване на IPS и защита от Malware в защитна стена FPR4115-NGFW-K9. Номер на договора за правото на ползване и поддръжка - 203500349	2	06.11.2025	31.12.2028
REQ.32.	ST-FR-LIC	Flow Rate лиценз за Cisco Secure Network Analytics. Номер на договора за правото на ползване и поддръжка - Sub1342345	17000	17.10.2027	31.12.2028
REQ.33.	L-LC-TI-FC4K=	Threat Feed лиценз за Cisco Secure Network Analytics. Номер на договора за правото на ползване и поддръжка - 205047243	1	17.10.2027	31.12.2028
REQ.34.	L-AC-APX-LIC=	Потребителски VPN лицензи Premier за софтуер Cisco Secure Client. Номер на договора за правото на ползване и поддръжка - 203184175	1000	31.08.2027	31.12.2028
REQ.35.	TGA-LIC-K9	Лиценз за sandbox система Cisco Secure Malware Analytics, който позволява до 500 семпъла дневно.	1	11.07.2027	31.12.2028

№	Вид или продуктов номер	Описание	Брой	Период на текуща валидност до:	Период на валидност до:
		Номер на договора за правото на ползване и поддръжка - Sub1289325			
REQ.36.	UMB-DNS-ADV-K9	Потребителски лиценз DNS Security Advantage за използване на облачна услуга за сигурност Cisco Umbrella. Номер на договора за правото на ползване и поддръжка - Sub1289326	8300	31.08.2027	31.12.2028

2. Поддейност 1.2.: Осигуряване на нови комуникационни устройства, софтуерни лицензи и поддръжка:

В обхвата на тази поддейност изпълнителят трябва да достави оборудване, което следва да отговаря на минималните изисквания, посочени в Таблиците от № 3 до № 13 по-долу:

1. SD-WAN рутер – 2 броя

Таблица № 3

Позиция	Минимални изисквания
Шаси и захранване	
REQ.1.	Захранване –модулно, 100 до 240 VAC, с два токозахранващи модула за резервиране.
Интерфейси:	
REQ.2.	12 интерфейса SFP+, които поддържат 10GE и 1GE модули.
REQ.3.	Ethernet интерфейс за управление и наблюдение.
REQ.4.	Брой USB 3.0 интерфейси – 1.
REQ.5.	Сериен конзолен интерфейс – 1.
Производителност	
REQ.6.	Пропускателна SDWAN способност от 20Gbps с IMIX трафична композиция.
REQ.7.	DRAM – 16GB с възможност за увеличаване до 64GB.

Позиция	Минимални изисквания
REQ.8.	SDWAN Overlay тунели – 8000.
SDWAN функции	
REQ.9.	Изграждане на SDWAN мрежа под управление на SDWAN контролери.
REQ.10.	Отделни control plane и data plane.
REQ.11.	Поддържа IPv4 и IPv6 WAN транспортни мрежи.
REQ.12.	Изграждането на SDWAN overlay с използването на един от следните протоколи- IPSec, GRE, LISP или еквивалентен протокол.
REQ.13.	AES-256 GCM алгоритъм за криптиране на трафика.
REQ.14.	Изграждане на стандартни IPsec с IKEv2 тунели до устройства на други производители.
REQ.15.	Уникална двойка ключове за всеки IPSec тунел в SDWAN мрежата – IPSec pairwise keys.
REQ.16.	Поддръжка на GRE over IPSec.
REQ.17.	TLS или DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите.
REQ.18.	Удостоверяване на идентичност между контролерите и рутерите с цифрови сертификати.
REQ.19.	Хардуерно базиран криптографски метод за удостоверяване на софтуерната автентичност.
REQ.20.	Използване на сертификати от CA на възложителя.
REQ.21.	Използване на сертификати от CA на производителя.
REQ.22.	AES-256 GCM алгоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета, на данните.
REQ.23.	Изолиране на трафика и маршрутизиращите таблици за определени вътрешни IP събнети чрез използване на един от следните методи - VRF, VRF Lite или еквивалентен метод за сегментация.
REQ.24.	Сегментиран пренос на трафика от вътрешни събнети през транспортните SDWAN тунели чрез MPLS маркери (tags) или еквивалентни технологии.
REQ.25.	Автоматично измерване на packet loss, jitter и delay за всеки SDWAN транспортен тунел.
REQ.26.	Автоматично маршутизиране на трафика, на ниво приложения и групи от приложения, през различни SDWAN тунели на база динамичните параметри на тунелите и политики – packet loss, jitter и delay.
REQ.27.	Вграден application firewall.
REQ.28.	Филтриране на трафика чрез ACL.

Позиция	Минимални изисквания
REQ.29.	Автоматично откриване на SDWAN контролерите без първоначална конфигурация чрез използването на DNS - plug-and-play, zero touch plug&play или еквивалентни методи.
REQ.30.	L3 overlay с управляеми L3 транспортни топологии – hub-and-spoke, full mesh и комбинации между двете.
REQ.31.	Управляема виртуална топология за всеки сегмент.
REQ.32.	L2 overlay, който поддържа poin-to-point и hub-and-spoke топологии.
REQ.33.	Рутинг протоколи за интеграция с външни мрежи: - RIP - OSPF - BGP - IS-IS - VRRP
REQ.34.	Функция gateway tracking или еквивалент.
REQ.35.	802.1Q VLAN.
REQ.36.	Service side NAT.
REQ.37.	Transport side NAT.
REQ.38.	Application-level gateway (ALG) NAT за SIP.
REQ.39.	Direct Internet Access (DIA) базиран на политики.
REQ.40.	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 SDWAN тунел. - QoS на ниво VPN/VRF сегмент.
REQ.41.	Packet duplication – изпращане на един пакет по два отделни маршрута до приемащия SD-WAN рутер.
REQ.42.	Forward Error Correction (FEC).
REQ.43.	Автоматичен избор на най-добрия маршрут до M365 приложения чрез измерване на закъснението и загубата на пакети от различни SDWAN рутери през Internet.
REQ.44.	Висока надеждност чрез съвместна работа с втори SDWAN рутер и използване на неговите WAN транспортни интерфейси за изграждане на SDWAN транспортни тунели.

Позиция	Минимални изисквания
REQ.45.	Multicast рутиране с поддръжка на IGMP v2, IGMP v3, PIM SSM и PIM ASM.
REQ.46.	Автоматична настройка на traffic shaping за всеки тунел на база загубите на пакети при преноса.
REQ.47.	Изграждане на динамични SDWAN overlay тунели.
Управление и наблюдение:	
REQ.48.	Протоколи и методи за управление и наблюдение: - Управление чрез SD-WAN контролери. - DHCP клиент. - DHCP сървър. - DNS. - NTP. - SNMP. - SSH. - Експортиране на трафична информация чрез един от следните протоколи - 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.
Гаранция, поддръжка и лицензи:	
REQ.49.	Хардуерна гаранция за срок до 31.12.2028г.
REQ.50.	Техническа поддръжка за срок до 31.12.2028г.
REQ.51.	Получаване на нови версии на софтуера за срок до 31.12.2028г.
REQ.52.	Лицензни абонаменти за използване на софтуерни функции за срок до 31.12.2028г.

2. DC комутатор - 10 броя

Таблица № 4

Позиция	Минимални изисквания
Шаси/кутия и захранване	
REQ.1.	Тип на кутията/шасито - за директен монтаж в 19“ шкаф максимум 1RU.
REQ.2.	Да поддържат захранване от 220-240v AC, 50Hz.
REQ.3.	Работен температурен диапазон от 0º до +40 ºC.
REQ.4.	Работна относителна влажност от до 85% .
REQ.5.	Въздушният поток да бъде в посока изхвърляне от портовете.
Общи изисквания за портовете:	

REQ.6.	Минимум 48 медни порта поддържащи 100M/1/2.5/5/10Gbps и 6 QSFP порта поддържащи 40/100Gbps.
REQ.7.	Брой USB портове - минимум 1.
REQ.8.	Ethernet порт за управление - минимум 1.
REQ.9.	Сериен конзолен порт - минимум 1.
Сигурност и защита:	
REQ.10.	Да поддържа хардуерно базиран криптографски метод за удостоверяване на софтуерната автентичност.
REQ.11.	Да поддържа изолиране на потребителите от един и същ VLAN.
REQ.12.	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.13.	Да поддържа игнориране на BPDU пакети получавани от клиентски портове.
REQ.14.	Да подържа възможност за игнориране на STP root bridge информация през неоторизирани портове.
REQ.15.	Да има възможност за добавяне на IEEE 802.1ae на всичките си портове.
Производителност и услуги:	
REQ.16.	Хардуерно маршрутизиране и комутиране със следните параметри, като минимум: - Производителност – 2,16 Tbps. - Forwarding – 1 200 Mpps. - Брой IPv4 маршрута – 1 700 000. - Брой IPv4 и IPv6 маршрута – 850 000.
REQ.17.	Комутаторът да се окомплектова с максималното количество памет предвидено от производителя.
REQ.18.	MAC адреси – минимум 512 000.
REQ.19.	Да поддържа Jumbo frames от поне 9198 байта.
REQ.20.	Да поддържа минимум 3500 802.1Q VLAN.
REQ.21.	Spanning Tree – IEEE 802.1d, 802.1w и 802.1w
REQ.22.	Да поддържа следните протоколи за маршрутизация: - Статично маршрутизиране. - IGMPv2 и IGMPv3 snooping. - VRRP. - DHCP Relay. - Динамично маршрутизиране: RIPv2, OSPFv2, OSPFv3, IS-IS, BGP. - Маршутизиране на база политика (PBR). - PIM, MSDP, SSM мултикаст маршрутизация.

REQ.23.	Да поддържа NetFlow.
REQ.24.	Да поддържа VXLAN BGP EVPN, включително Multi-site.
REQ.25.	Да поддържа MPLS, MPLS L3 VPN, Inter AS (option B).
REQ.26.	Да поддържа IEEE 802.3ad LACP протокол.
REQ.27.	Да поддържа MLAG.
REQ.28.	Да поддържа LLDP.
REQ.29.	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.
Управление и наблюдение:	
REQ.30.	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.31.	Устройството да може да се администрира от съществуващите Cisco APIC контролери в режим ACI.
REQ.32.	Устройството да може да се наблюдава от съществуващата система Cisco Nexus Dashboard Insights в пълната си функционалност.
REQ.33.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя за обезпечаване на описаните по-горе функции.
Гаранция, поддръжка и лицензи:	
REQ.34.	Хардуерна гаранция за срок от 5 (пет) години.
REQ.35.	Техническа поддръжка за срок от 5 (пет) години.
REQ.36.	Получаване на нови версии на софтуера за срок от 5 (пет) години.
REQ.37.	Лицензни абонаменти за използване на софтуерни функции за срок от 5 (пет) години.

3. SAN комутатор - 2 броя

Таблица № 5

Позиция	Минимални изисквания
Шаси/кутия и захранване	
REQ.1.	Тип на кутията/шасито - за директен монтаж в 19“ шкаф максимум 2RU.
REQ.2.	Да поддържат захранване от 220-240v AC, 50Hz.
REQ.3.	Работен температурен диапазон от 0º до +40 ºC.
REQ.4.	Работна относителна влажност от до 85% .
REQ.5.	Въздушният поток да бъде в посока изхвърляне от портовете.
Основни функции	
REQ.6.	Да има минимум 64 Fibre Channel порта оборудвани с 8/16/32 Gbit/s SFP модула за работа на разстояние до 100 метра върху OM3/OM4 мултимод кабел (две влакна).
REQ.7.	Да може да бъде разширен с допълнителни 32 порта работещи на скорост до 32 Gbit/s.

REQ.8.	Комутаторът трябва да поддържа възможност за ограничаване на достъпа до интерфейса за управление чрез IPv4/IPv6 правила за достъп (ACLs).
REQ.9.	Портовете на Комутаторът да поддържат следните скорости: 4, 8, 16, 32Gbit/s.
REQ.10.	Архитектурата на Комутаторът да позволява работата му на пълна скорост на всички портове.
REQ.11.	Комутаторът да поддържа възможност за обновяване на софтуера, без това да прекъсва работата на устройството.
REQ.12.	Комутаторът да поддържа автоматизация на обновяването на операционната системата и инсталацията на конфигурационния файл при имплементацията на нов комутатор.
REQ.13.	Комутаторът да поддържа изграждането на ISL от група от портове.
REQ.14.	Комутаторът да поддържа използването на поне 16 порта в такава ISL група.
REQ.15.	Комутаторът да поддържа разделянето на фабриката на отделни виртуални SAN мрежи/фабрики.
REQ.16.	Комутаторът да поддържа NPV (N_Port Virtualization).
REQ.17.	Комутаторът да бъде доставен с възможност за достигане на 8000 буфер кредита на порт.
REQ.18.	Комутаторът трябва да има възможност да отстраняване на повредени фреймове на базата на CRC проверка.
REQ.19.	Комутаторът да поддържа рестартиране на процес със запазване на състоянието.
REQ.20.	Комутаторът да поддържа хардуерно базиран криптографски метод за удостоверяване на софтуерната автентичност.
REQ.21.	Комутаторът да поддържа криптиране на Fibre Channel портовете.
REQ.22.	Комутаторът да поддържа маршрутизиране между виртуалните SAN мрежи.
REQ.23.	Комутаторът да поддържа Fibre Channel Security Protocol (FC-SP).
REQ.24.	Комутаторът да поддържа Zone-базиран QoS.
Управление и наблюдение:	
REQ.25.	Комутаторът да поддържа SSH.
REQ.26.	Комутаторът трябва да поддържа програмен интерфейс (RESTful API) на самото устройство.
Гаранция, поддръжка и лицензи:	
REQ.27.	Хардуерна гаранция за срок до 31.12.2028г.
REQ.28.	Техническа поддръжка за срок до 31.12.2028г.
REQ.29.	Получаване на нови версии на софтуера за срок до 31.12.2028г.

REQ.30.	Лицензни абонаменти за използване на софтуерни функции за срок до 31.12.2028г.

4. Система за централизирано автентикиране на потребители (Виртуален аплайънс) – 2 броя

Таблица № 6

Позиция	Минимални изисквания
Основни функции	
REQ.1.	Виртуалният аплайънс да поддържа следните хипервайзори: • VMware ESXi • Linux KVM • Microsoft Hyper-V
REQ.2.	Да поддържат минимум 10 000 потребителя.
REQ.3.	Да позволява миграция на политиките за достъп до мрежата от съществуващите хардуерни аплайънси Cisco SNS 3655.
REQ.4.	Да позволяват версия на Cisco ISE 3.x.
REQ.5.	Да са съвместими със съществуващите лицензи на Cisco ISE.
Гаранция, поддръжка и лицензи:	
REQ.6.	Техническа поддръжка за срок до 31.12.2028г.
REQ.7.	Получаване на нови версии на софтуера за срок до 31.12.2028г.
REQ.8.	Лицензни абонаменти за използване на софтуерни функции за срок до 31.12.2028г.

5. Система за централизирано управление на защитни стени (Виртуален аплайънс) – 1 брой

Таблица № 7

Позиция	Минимални изисквания
Основни функции	
REQ.1.	Виртуалният аплайънс да поддържа следните хипервайзори: • VMware ESXi • Linux KVM • Microsoft Hyper-V
REQ.2.	Да позволява миграция на политиките за достъп до мрежата от съществуващият хардуерен аплайънс Cisco FMC 1600.
REQ.3.	Да поддържа управлението на минимум 300 хардуерни и виртуални защитни стени.

REQ.4.	Да има минимум 2TB пространство за съхраняване на логове.
REQ.5.	Да позволяват версия на Cisco FMC 7.x.
REQ.6.	Да са съвместими със съществуващите защитни стени Cisco 4115, както и с такива предложени като подмяна.
Гаранция, поддръжка и лицензи:	
REQ.7.	Техническа поддръжка за срок до 31.12.2028г.
REQ.8.	Получаване на нови версии на софтуера за срок до 31.12.2028г.
REQ.9.	Лицензни абонаменти за използване на софтуерни функции за срок до 31.12.2028г.

6. Защитна стена – 2 броя

Таблица № 8

Позиция	**Минимални изисквания**
Шаси/кутия и захранване	
REQ.1.	Тип на кутията/шасито - за директен монтаж в 19“ шкаф максимум 1RU.
REQ.2.	Да поддържат захранване от 220-240v AC, 50Hz.
REQ.3.	Работен температурен диапазон от 0º до +40 ºC.
REQ.4.	Работна относителна влажност от до 85% .
Общи изисквания за портовете:	
REQ.5.	Минимум осем броя 1GE RJ45 интерфейса.
REQ.6.	Минимум осем броя 1/10GE SFP+ интерфейса с възможност за разширение до 16.
REQ.7.	Брой USB портове - минимум 1 брой.
REQ.8.	Да има отделни Ethernet и сериен RS-232 интерфейси за управление.
Производителност и услуги:	
REQ.9.	Производителност: - минимум 20 Gbps със работещи statefull inspection firewall, IPS и deep packet inspection (1024B пакети). - брой сесии – минимум 4 000 000. - нови сесии за 1 секунда - минимум 150 000. - IPSec производителност – минимум 12 Gbps. - Производителност на TLS декриптиране – минимум 5 Gbps. - VPN тунели – минимум 6 000.
REQ.10.	Да поддържа прозрачен режим на работа – Inline.
REQ.11.	Да поддържа режим на работа като маршрутизатор.

REQ.12.	Да поддържа IPSec тунели с IKE/IKEv2 управление на сесиите и следните методи за защита: - Encryption: 3DES, AES-128 и AES-256. - Authentication: preshared key, RSA и ECDSA. - Integrity: SHA, SHA-256, SHA-384, SHA-512.
REQ.13.	Да поддържа SCEP протокол за получаване на сертификат.
REQ.14.	Да поддържа OCSP за проверка валидността на сертификати.
REQ.15.	Да поддържа декриптиране на трафик за инспекция.
REQ.16.	Да има възможност за добавяне на SSL VPN клиенти.
REQ.17.	Да поддържа 802.1Q VLAN.
REQ.18.	Да има вградена IPS система.
REQ.19.	Да има вградена Anti-Malware система за защита от файлове със зловреден код.
REQ.20.	Да поддържа ретроспективно уведомяване на администратора при получаване на нова информация, която класифицира вече свалени файлове като съдържащи зловреден код.
REQ.21.	Да има възможност за добавяне на категоризация на Web URL на база категории и ниво на риска.
REQ.22.	Да има вградена DPI система с класифициране на мрежовия трафик на ниво приложения и категории от приложения.
REQ.23.	Да поддържа минимум следните протоколи за маршрутизация: - RIP и RIPv2 - OSPFv2 и OSPFv3 - BGPv4
REQ.24.	Да поддържа минимум IGMPv2 и PIM-SM мултикаст маршрутизиране.
REQ.25.	Да поддържа динамичен и статичен NAT.
REQ.26.	Да поддържа динамичен и статичен PAT.
REQ.27.	Да поддържа минимум следните PAT и NAT услуги: - NAT за IPv4 - NAT 66 - NAT 64/46 транслации
REQ.28.	Да поддържа NAT AGL за SIP, H.323 и FTP протоколи.
REQ.29.	Да позволява обособяване на DMZ зони.
REQ.30.	Да поддържа rate limiting с класифициране на трафика на база минимум следните параметри: - Интерфейс - IP мрежи - Приложения и категории от приложения - URL категория и репутация

	- Active Directory потребители и групи от потребители
REQ.31.	Да поддържа интеграция с Microsoft Active Directory за идентификация на потребителите и създаването на Firewall политики на база AD групи и потребителите.
REQ.32.	Да поддържа идентификация на потребителите чрез външен RADIUS сървър.
REQ.33.	Да поддържа active-standby HA режим на работа.
REQ.34.	Да поддържа active-active HA режим на работа до осем устройства в паралел.
REQ.35.	Да поддържа хардуерно базиран криптографски метод за удостоверяване на софтуерната автентичност.
Управление и наблюдение:	
REQ.36.	Да поддържа минимум следните методи за управление и наблюдение: - Конзола, HTTP и HTTPS. - Ping - DNS - NTP - SSHv2c и SNMPv3 - Syslog - Експортиране на трафична информация чрез IPFIX, Netflow, Jflow или подобен протокол към външна система за трафичен анализ. - Идентификация на администратрите чрез локална база, RADIUS сървър и LDAP. - Отделен Ethernet порт за out of band управление и наблюдение на устройството.
REQ.37.	Устройството да има инсталирана и лицензирана с постоянен лиценз операционна система.
REQ.38.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя.
Гаранция, поддръжка и лицензи:	
REQ.39.	Хардуерна гаранция за срок до 31.12.2028г.
REQ.40.	Техническа поддръжка за срок до 31.12.2028г.
REQ.41.	Получаване на нови версии на софтуера за срок до 31.12.2028г.
REQ.42.	Лицензни абонаменти за използване на софтуерни функции за срок до 31.12.2028г.

7. Комутатор с 24 порта 1GE, L3 и PoE – 16 броя

Таблица № 9

Позиция	Минимални изисквания
Шаси и захранване:	
REQ.1.	Монтаж - в 19“ шкаф.
REQ.2.	Токозахранване – модулно, 100-240VAC, с два токозахранващи модула за резервиране.
REQ.3.	24 порта 100/1000BASE-T и 8 порта SFP+, които поддържат 1GE и 10GE модули
REQ.4.	Стеково свързване с производителност 400Gbps.
REQ.5.	Изграждане на стек от 8 комутатора.
REQ.6.	Обща захранваща шина за споделяне на захранването между 4 комутатора.
REQ.7.	802.3af и 802.3at PoE с обща мощност 720W.
REQ.8.	Осигуряване на PoE захранване без прекъсване при рестарт на комутатора.
REQ.9.	USB порт.
REQ.10.	Сериен конзолен порт.
REQ.11.	Хардуерно IP forwarding и комутиране със следните параметри: - Производителност - 20Gbps. - Forwarding – 150Mpps. - MAC адреси – 32000. - IPv4 маршрути – 32000. - IPv6 маршрути – 16000. - Мултикаст маршрути – 8000. - SVI интерфейси – 1000. - Пакетни буфери – 16MB.
REQ.12.	DRAM - 8GB.
REQ.13.	802.1AE с 256 битово криптиране и MKA.
REQ.14.	Jumbo frames - 9198 байта.
REQ.15.	Експортиране на трафична информация за 64000 трафични потока чрез един от следните протоколи - IPFIX, NetFlow, JFlow, sFlow или еквивалентен протокол.
REQ.16.	Statefull Switch Over (SSO) между комутатори в един стек за следните функции: - Рутиране. - STP. - 802.3ad.

Позиция	Минимални изисквания
REQ.17.	Spanning Tree – IEEE 802.1d, 802.1w и 802.1s.
REQ.18.	Разпознаване на мрежова връзка с еднопосочна пропускливост между два комутатора от същия вид.
REQ.19.	Класифициране на трафичните потоци на ниво приложение.
REQ.20.	Копиране на трафика от един порт към друг– Port mirroring или еквивалентна функция.
REQ.21.	Копиране на трафика от един порт към друг през L3 мрежа.
REQ.22.	Non stop forwarding (NSF) или еквивалентна функция.
REQ.23.	Рутинг протоколи: - RIPv2. - OSPF и OSPFv3. - IS-ISv4. - BGPv4 и BGPv6. - IGMP и IGMPv3. - PIM SM мултикаст рутиране - VRRP. - Рутиране на база политики. - VRF Lite или еквивалент.
REQ.24.	MPLS с L2 и L3 VPN функционалност.
REQ.25.	BGP EVPN с VXLAN за изграждане на фабрика, която е базирана на отворени стандарти.
REQ.26.	IEEE 802.3ad LACP протокол.
REQ.27.	IEEE 802.3ad групи с портове от различни комутатори в един стек.
REQ.28.	IEEE 802.1AB (LLDP) и LLDP-MED.
REQ.29.	QoS със следните функции: - HQoS. - 8 изходящи пакетни опашки на всеки порт. - 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. - Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всеки клас от общата пропускателна способност на интерфейса. - 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.

Позиция	Минимални изисквания
Сигурност:	
REQ.30.	Изолиране на потребителите от един и същ VLAN.
REQ.31.	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. • 802.1x идентификация на повече от едно устройство на комутаторен порт. • 802.1x Multi-Domain идентификация.
REQ.32.	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.33.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимален брой пакети в секунда
REQ.34.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимална скорост в секунда.
REQ.35.	DHCP Snooping или еквивалентен метод.
REQ.36.	DHCP опция 82.
REQ.37.	Dynamic ARP inspection или еквивалентен метод.
REQ.38.	IP source guard или еквивалентен метод за защита от IP spoofing в мрежи с динамично и статично присвояване на IP адресите.
REQ.39.	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.40.	Spanning Tree защити - BPDU Guard и Root Guard.
REQ.41.	Хардуерен модул за удостоверяване автентичността на хардуера и софтуера чрез използване на криптографски методи.
Управление и наблюдение:	
REQ.42.	Протоколи и функции за управление и наблюдение: - Web GUI. - CLI. - DNS. - TFTP. - FTP. - NTP. - SSHv2 и SNMPv3. - Вграден DHCP сървър.

Позиция	Минимални изисквания
	- 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. - API интерфейс с поддръжка на gNMI, RESTCONF и NETCONF. - YANG дейта модели.
Гаранция, поддръжка и лицензи:	
REQ.43.	Хардуерна гаранция за срок от 5 (пет) години.
REQ.44.	Техническа поддръжка за срок от 5 (пет) години.
REQ.45.	Получаване на нови версии на софтуера за срок от 5 (пет) години.
REQ.46.	Лицензни абонаменти за използване на софтуерни функции за срок от 5 (пет) години.

8. Комутатор с 48 порта 1GE, L3 и PoE – 12 броя

Таблица № 10

Позиция	Минимални изисквания
Шаси и захранване:	
REQ.1.	Монтаж - в 19“ шкаф.
REQ.2.	Токозахранване – модулно, 100-240VAC, с два токозахранващи модула за резервиране.
Портове:	
REQ.3.	48 порта 100/1000BASE-T и 8 порта SFP+, които поддържат 1GE и 10GE модули.
REQ.4.	Стеково свързване с производителност 400Gbps.
REQ.5.	Изграждане на стек от 8 комутатора.
REQ.6.	Обща захранваща шина за споделяне на захранването между 4 комутатора.
REQ.7.	802.3af и 802.3at PoE с обща мощност 1100W.
REQ.8.	Осигуряване на PoE захранване без прекъсване при рестарт на комутатора.
REQ.9.	USB порт.
REQ.10.	Сериен конзолен порт.
Производителност и услуги:	
REQ.11.	Хардуерно IP forwarding и комутиране със следните параметри: - Производителност - 250Gbps. - Forwarding – 180Mpps. - MAC адреси – 32000.

	- IPv4 маршрути – 32000. - IPv6 маршрути – 16000. - Мултикаст маршрути – 8000. - SVI интерфейси – 1000. - Пакетни буфери – 16MB.
REQ.12.	DRAM - 8GB.
REQ.13.	802.1AE с 256 битово криптиране и MKA..
REQ.14.	Jumbo frames - 9198 байта.
REQ.15.	Копиране на трафика от порт – Port mirroring или еквивалентна функция.
REQ.16.	Експортиране на трафична информация за 64000 трафични потока чрез един от следните протоколи - IPFIX, NetFlow, JFlow, sFlow или еквивалентен протокол.
REQ.17.	Statefull Switch Over (SSO) между комутатори в един стек за следните функции: - Рутиране. - STP. - 802.3ad.
REQ.18.	Spanning Tree – IEEE 802.1d, 802.1w и 802.1s.
REQ.19.	Разпознаване на мрежова връзка с еднопосочна пропускливост между два комутатора от същия вид.
REQ.20.	Класифициране на трафичните потоци на ниво приложение.
REQ.21.	Копиране на трафика от един порт към друг– Port mirroring или еквивалентна функция.
REQ.22.	Копиране на трафика от един порт към друг през L3 мрежа.
REQ.23.	Non stop forwarding (NSF) или еквивалентна функция.
REQ.24.	Рутинг протоколи: - RIPv2. - OSPF и OSPFv3. - IS-ISv4. - BGPv4 и BGPv6. - IGMP и IGMPv3. - PIM SM мултикаст рутиране - VRRP. - Рутиране на база политики. - VRF Lite или еквивалент.
REQ.25.	MPLS с L2 и L3 VPN функционалност.
REQ.26.	BGP EVPN с VXLAN за изграждане на фабрика, която е базирана на отворени стандарти.
REQ.27.	IEEE 802.3ad LACP протокол.
REQ.28.	IEEE 802.3ad групи с портове от различни комутатори в един стек.

REQ.29.	IEEE 802.1AB (LLDP) и LLDP-MED.
REQ.30.	QoS със следните функции: - HQoS. - 8 изходящи пакетни опашки на всеки порт. - 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. - Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всеки клас от общата пропускателна способност на интерфейса. - 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.
Сигурност:	
REQ.31.	Изолиране на потребителите от един и същ VLAN.
REQ.32.	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. • 802.1x идентификация на повече от едно устройство на комутаторен порт. • 802.1x Multi-Domain идентификация.
REQ.33.	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.34.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимален брой пакети в секунда
REQ.35.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимална скорост в секунда.
REQ.36.	DHCP Snooping или еквивалентен метод.
REQ.37.	DHCP опция 82.
REQ.38.	Dynamic ARP inspection или еквивалентен метод.
REQ.39.	IP source guard или еквивалентен метод за защита от IP spoofing в мрежи с динамично и статично присвояване на IP адресите.

REQ.40.	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.41.	Spanning Tree защити - BPDU Guard и Root Guard.
REQ.42.	Хардуерен модул за удостоверяване автентичността на хардуера и софтуера чрез използване на криптографски методи.
Управление и наблюдение:	
REQ.43.	Протоколи и функции за управление и наблюдение: - Web GUI. - CLI. - DNS. - TFTP. - FTP. - NTP. - SSHv2 и SNMPv3. - Вграден DHCP сървър. - 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. - API интерфейс с поддръжка на gNMI, RESTCONF и NETCONF. - YANG дейта модели.
Гаранция, поддръжка и лицензи:	
REQ.44.	Хардуерна гаранция за срок от 5 (пет) години.
REQ.45.	Техническа поддръжка за срок от 5 (пет) години.
REQ.46.	Получаване на нови версии на софтуера за срок от 5 (пет) години.
REQ.47.	Лицензни абонаменти за използване на софтуерни функции за срок от 5 (пет) години.

9. Комутатор с 12 порта 1GE, L3 и PoE – 30 броя

Таблица № 11

Позиция	**Минимални изисквания**
Шаси и захранване:	
REQ.1.	Токозахранване – вградено, 100-240VAC..
REQ.2.	Безшумна работа.
REQ.3.	Слот за SD карта.
Портове:	

Позиция	Минимални изисквания
REQ.4.	12 порта 100/1000BASE-T, два ъплинк порта 1000BASE-T и два ъплинк порта SFP+ (10GE).
REQ.5.	802.3af и 802.3at PoE с обща мощност 240W.
REQ.6.	Осигуряване на PoE захранване без прекъсване при рестарт на комутатора.
REQ.7.	USB порт.
REQ.8.	Конзолен порт.
Производителност и услуги:	
REQ.9.	Хардуерно IP forwarding и комутиране със следните параметри: - Производителност - 68Gbps. - Forwarding – 50Mpps. - MAC адреси – 32000. - IPv4 маршрути – 4000. - IPv6 маршрути – 2000. - Мултикаст маршрути – 1000. - SVI интерфейси – 512. - Пакетни буфери – 6MB.
REQ.10.	DRAM - 4GB.
REQ.11.	802.1AE с 256 битово криптиране.
REQ.12.	Jumbo frames - 9198 байта.
REQ.13.	Експортиране на трафична информация за 16000 трафични потока чрез един от следните протоколи - IPFIX, NetFlow, JFlow, sFlow или еквивалентен протокол.
REQ.14.	Spanning Tree – IEEE 802.1d, 802.1w и 802.1s.
REQ.15.	Разпознаване на мрежова връзка с еднопосочна пропускливост между два комутатора от същия вид.
REQ.16.	Класифициране на мрежовите потоци на ниво приложение.
REQ.17.	Рутинг протоколи: - RIPv2 и RIPng. - OSPF и OSPFv3. - IS-ISv4. - IGMP и IGMPv3. - PIM SM мултикаст рутиране. - VRRP. - Рутиране на база политики. - VRF Lite или еквивалент.
REQ.18.	IEEE 802.3ad LACP протокол.
REQ.19.	IEEE 802.1AB (LLDP) и LLDP-MED.
REQ.20.	QoS със следните функции:

Позиция	Минимални изисквания
	- HQoS. - 8 изходящи пакетни опашки на всеки порт. - 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. - Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всеки клас от общата пропускателна способност на интерфейса. - 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.
Сигурност:	
REQ.21.	Изолиране на потребителите от един и същ VLAN.
REQ.22.	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. • 802.1x идентификация на повече от едно устройство на комутаторен порт. • 802.1x Multi-Domain идентификация.
REQ.23.	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.24.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимален брой пакети в секунда
REQ.25.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимална скорост в секунда.
REQ.26.	DHCP Snooping или еквивалентен метод.
REQ.27.	DHCP опция 82.
REQ.28.	Dynamic ARP inspection или еквивалентен метод.
REQ.29.	IP source guard или еквивалентен метод за защита от IP spoofing в мрежи с динамично и статично присвояване на IP адресите.
REQ.30.	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.

Позиция	Минимални изисквания
REQ.31.	Spanning Tree защити - BPDU Guard и Root Guard.
REQ.32.	Хардуерен модул за удостоверяване автентичността на хардуера и софтуера чрез използване на криптографски методи.
Управление и наблюдение:	
REQ.33.	Протоколи и функции за управление и наблюдение: - Web GUI. - CLI. - DNS. - TFTP. - FTP. - NTP. - SSHv2 и SNMPv3. - Вграден DHCP сървър. - Traffic policing за контролиране на трафика до контролната система на комутатора. - Идентификация на администраторите чрез външни RADIUS и TACACS+ системи. - API интерфейс с поддръжка на RESTCONF и NETCONF. - YANG дейта модели.
Гаранция, поддръжка и лицензи:	
REQ.34.	Хардуерна гаранция за срок от 5 (пет) години.
REQ.35.	Техническа поддръжка за срок от 5 (пет) години.
REQ.36.	Получаване на нови версии на софтуера за срок от 5 (пет) години.
REQ.37.	Лицензни абонаменти за използване на софтуерни функции за срок от 5 (пет) години.

10. Комутатор с 24 порта 1GE и PoE – 30 броя

Таблица № 12

Позиция	Минимални изисквания
Шаси и захранване:	
REQ.1.	Монтаж - в 19“ шкаф.
REQ.2.	Токозахранване – модулно, 100-240VAC, с два токозахранващи модула за резервиране.
Портове:	
REQ.3.	24 порта 100/1000BASE-T и четири порта SFP+ (10GE).

Позиция	Минимални изисквания
REQ.4.	Възможност за добавяне на стеково свързване с производителност 80Gbps и изграждане на стек до осем комутатора.
REQ.5.	802.3af и 802.3at PoE с обща мощност 740W.
REQ.6.	Осигуряване на PoE захранване без прекъсване при рестарт на комутатора.
REQ.7.	USB порт.
REQ.8.	Сериен конзолен порт.
Производителност и услуги:	
REQ.9.	Хардуерно IP forwarding и комутиране със следните параметри: - Производителност - 128Gbps. - Forwarding – 95Mpps. - MAC адреси – 16000. - IPv4 маршрути – 3000. - IPv6 маршрути – 1500. - SVI интерфейси – 512. - Пакетни буфери – 6MB.
REQ.10.	DRAM - 2GB.
REQ.11.	802.1AE с 128 битово криптиране.
REQ.12.	Jumbo frames - 9198 байта.
REQ.13.	Експортиране на трафична информация за 16000 трафични потока чрез един от следните протоколи - IPFIX, NetFlow, JFlow, sFlow или еквивалентен протокол.
REQ.14.	Statefull Switch Over (SSO) между комутатори в един стек за следните функции: - Рутиране. - STP. - 802.3ad.
REQ.15.	Spanning Tree – IEEE 802.1d, 802.1w и 802.1s.
REQ.16.	Разпознаване на мрежова връзка с еднопосочна пропускливост между два комутатора от същия вид.
REQ.17.	Рутинг протоколи: - RIPv2. - OSPF с 1000 маршрута. - IGMP. - VRRP. - Рутиране на база политики.
REQ.18.	Възможност за добавяне на IS-ISv4.
REQ.19.	Възможност за добавяне на VRF Lite или еквивалент.
REQ.20.	Възможност за добавяне на PIM SM мултикаст рутиране.
REQ.21.	IEEE 802.3ad LACP протокол.

Позиция	Минимални изисквания
REQ.22.	IEEE 802.3ad групи с портове от различни комутатори в един стек.
REQ.23.	IEEE 802.1AB (LLDP) и LLDP-MED.
REQ.24.	QoS със следните функции: - HQoS. - 8 изходящи пакетни опашки на всеки порт. - 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. - Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всеки клас от общата пропускателна способност на интерфейса. - 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.
Сигурност:	
REQ.25.	Изолиране на потребителите от един и същ VLAN.
REQ.26.	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. • 802.1x идентификация на повече от едно устройство на комутаторен порт. • 802.1x Multi-Domain идентификация.
REQ.27.	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.28.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимален брой пакети в секунда
REQ.29.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимална скорост в секунда.
REQ.30.	DHCP Snooping или еквивалентен метод.
REQ.31.	DHCP опция 82.
REQ.32.	Dynamic ARP inspection или еквивалентен метод.

Позиция	Минимални изисквания
REQ.33.	IP source guard или еквивалентен метод за защита от IP spoofing в мрежи с динамично и статично присвояване на IP адресите.
REQ.34.	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.35.	Spanning Tree защити - BPDU Guard и Root Guard.
REQ.36.	Хардуерен модул за удостоверяване автентичността на хардуера и софтуера чрез използване на криптографски методи.
Управление и наблюдение:	
REQ.37.	Протоколи и функции за управление и наблюдение: - Web GUI. - CLI. - DNS. - TFTP. - FTP. - NTP. - SSHv2 и SNMPv3. - Вграден DHCP сървър. - 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. - API интерфейс с поддръжка на RESTCONF и NETCONF. - YANG дейта модели.
Гаранция, поддръжка и лицензи:	
REQ.38.	Хардуерна гаранция за срок от 5 (пет) години.
REQ.39.	Техническа поддръжка за срок от 5 (пет) години.
REQ.40.	Получаване на нови версии на софтуера за срок от 5 (пет) години.
REQ.41.	Лицензни абонаменти за използване на софтуерни функции за срок от 5 (пет) години.

11. Комутатор с 48 порта 1GE и PoE – 10 броя

Таблица № 13

Позиция	Минимални изисквания
Шаси и захранване:	
REQ.1.	Монтаж - в 19“ шкаф.

Позиция	Минимални изисквания
REQ.2.	Токозахранване – модулно, 100-240VAC, с два токозахранващи модула за резервиране.
Портове:	
REQ.3.	48 порта 100/1000BASE-T и четири порта SFP+ (10GE).
REQ.4.	Възможност за добавяне на стеково свързване с производителност 80Gbps и изграждане на стек до осем комутатора.
REQ.5.	802.3af и 802.3at PoE с обща мощност 1400W.
REQ.6.	Осигуряване на PoE захранване без прекъсване при рестарт на комутатора.
REQ.7.	USB порт.
REQ.8.	Сериен конзолен порт.
Производителност и услуги:	
REQ.9.	Хардуерно IP forwarding и комутиране със следните параметри: - Производителност - 176Gbps. - Forwarding – 130Mpps. - MAC адреси – 16000. - IPv4 маршрути – 3000. - IPv6 маршрути – 1500. - SVI интерфейси – 512. - Пакетни буфери – 6MB.
REQ.10.	DRAM - 2GB.
REQ.11.	802.1AE с 128 битово криптиране.
REQ.12.	Jumbo frames - 9198 байта.
REQ.13.	Експортиране на трафична информация за 16000 трафични потока чрез един от следните протоколи - IPFIX, NetFlow, JFlow, sFlow или еквивалентен протокол.
REQ.14.	Statefull Switch Over (SSO) между комутатори в един стек за следните функции: - Рутиране. - STP. - 802.3ad.
REQ.15.	Spanning Tree – IEEE 802.1d, 802.1w и 802.1s.
REQ.16.	Разпознаване на мрежова връзка с еднопосочна пропускливост между два комутатора от същия вид.
REQ.17.	Рутинг протоколи: - RIPv2. - OSPF с 1000 маршрута. - IGMP. - VRRP. - Рутиране на база политики.

Позиция	Минимални изисквания
REQ.18.	Възможност за добавяне на IS-ISv4.
REQ.19.	Възможност за добавяне на VRF Lite или еквивалент.
REQ.20.	Възможност за добавяне на PIM SM мултикаст рутиране.
REQ.21.	IEEE 802.3ad LACP протокол.
REQ.22.	IEEE 802.3ad групи с портове от различни комутатори в един стек.
REQ.23.	IEEE 802.1AB (LLDP) и LLDP-MED.
REQ.24.	QoS със следните функции: - HQoS. - 8 изходящи пакетни опашки на всеки порт. - 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. - Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всеки клас от общата пропускателна способност на интерфейса. - 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.
Сигурност:	
REQ.25.	Изолиране на потребителите от един и същ VLAN.
REQ.26.	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. • 802.1x идентификация на повече от едно устройство на комутаторен порт. • 802.1x Multi-Domain идентификация.
REQ.27.	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.28.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимален брой пакети в секунда
REQ.29.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимална скорост в секунда.

Позиция	Минимални изисквания
REQ.30.	DHCP Snooping или еквивалентен метод.
REQ.31.	DHCP опция 82.
REQ.32.	Dynamic ARP inspection или еквивалентен метод.
REQ.33.	IP source guard или еквивалентен метод за защита от IP spoofing в мрежи с динамично и статично присвояване на IP адресите.
REQ.34.	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.35.	Spanning Tree защити - BPDU Guard и Root Guard.
REQ.36.	Хардуерен модул за удостоверяване автентичността на хардуера и софтуера чрез използване на криптографски методи.
Управление и наблюдение:	
REQ.37.	Протоколи и функции за управление и наблюдение: - Web GUI. - CLI. - DNS. - TFTP. - FTP. - NTP. - SSHv2 и SNMPv3. - Вграден DHCP сървър. - 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. - API интерфейс с поддръжка на RESTCONF и NETCONF. - YANG дейта модели.
Гаранция, поддръжка и лицензи:	
REQ.38.	Хардуерна гаранция за срок от 5 (пет) години.
REQ.39.	Техническа поддръжка за срок от 5 (пет) години.
REQ.40.	Получаване на нови версии на софтуера за срок от 5 (пет) години.
REQ.41.	Лицензни абонаменти за използване на софтуерни функции за срок от 5 (пет) години.

III. Дейност 2: „Осигуряване на решение за виртуализация, хардуерна и софтуерна поддръжка на оборудване и доставка на ново допълнително прилежащо оборудване“

1. Поддейност 2.1.: Осигуряване на решение за виртуализация

1.1 Обхват на услугата

Услугата обхваща осигуряване на лиценз за право на ползване и поддръжка на софтуер за виртуализация.

В Таблица № 14 са описани минималните изисквания по отношение на осигуряване на лиценз за право на ползване и поддръжка на софтуер за виртуализация – Vmware.

Таблица № 14

Вид софтуер	Описание	Количество	Валидност на текуща поддръжка до:	Осигурено право на ползване и поддръжка до:
Софтуер за виртуализация	VMware vSphere Foundation 8	1280 ядра	25.09.2025г.	24.09.2028г.

1.2 Параметри на услугата

Осигуряването на правото на ползване и поддръжката на софтуерните лицензи, включени в обхвата на настоящата заявка, следва да осигури възможност за ползване на:

- всички включени актуализации и нови версии (Updates, Upgrades, Renewals & PlugIns) до най-новите характеристики и функционалност на съответния продукт за срока на поддръжката;
- всички включени добавки (Plug-in Modules) налични за съответния продукт за срока на поддръжката;
- всички включени поправки (Fixes & Patches, etc.) налични за съответния продукт за срока на поддръжката.

1.3 Изисквания към изпълнението

Изпълнителят следва да осигури лицензите от лице, надлежно оторизирано от производителя на софтуера или от негов официален представител за предоставено право на извършване на разпространение на предлаганите софтуерни продукти на територията на Република България.

2. Поддейност 2.2 „Подновяване на поддръжката на сървърни системи Dell“

2.1. *Обхват на услугата*

Настоящата услуга обхваща следната техника:

- Осигуряване на хардуерна и софтуерна поддръжка за следните видове продукти за срок, посочен в таблица № 15 по-долу:

Таблица № 15

Вид техника	Сериен номер	Брой	Валидност на текуща поддръжка до:	Осигуряване на поддръжка до:
Сървърно шаси „Dell PowerEdge MX 7000”	JRCHY53; 84KGY53;	2	25.09.2025г.	31.12.2030г.
Мрежови модули MX9116n	DLDGY53; 501JY53	2	25.09.2025г.	31.12.2030г.
Мрежови модули MX7116n	C9JHY53; F9JHY53;	2	25.09.2025г.	31.12.2030г.
Сървъри “Dell PowerEdge MX 740C”	9M2R8Q3; BM2R8Q3; 7M2R8Q3; 8M2R8Q3; 3PQGY53; CLDGY53; 4PQGY53; HRCHY53; 301JY53; BLDGY53; 401JY53; GRCHY53; J6WGY53; JJ5JY53; 17WGY53; 1K5JY53;	16	25.09.2025г.	31.12.2030г.

2.2. *Параметри на услугата*

- Възможност за регистриране на инциденти в сайта на производителя
- Възможност за изтегляне на актуализации от сайта на производителя
- Възможност за хардуерна поддръжка на място и замяна на дефектирал компонент

2.3. *Изисквания към изпълнението*

Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или негово официално представителство за правото на разпространение и гаранционна поддръжка на описаните хардуерни продукти на територията на Република България.

3. Поддейност 2.3 „Подновяване на поддръжката на дискова система IBM FS 9200“

3.1. *Обхват на услугата*

Осигуряване на хардуерна и софтуерна поддръжка за следното оборудване посочено в Таблица № 16:

Таблица №16

Вид техника	Сериен номер	Брой	Валидност на текуща поддръжка до:	Осигуряване на поддръжка до:
Дисков масиви IBM FS9200	78E325M	1	09.10.2025г.	31.12.2030г.

3.2. *Параметри на услугата*

- Възможност за регистриране на инциденти в сайта на производителя
- Възможност за изтегляне на актуализации от сайта на производителя
- Възможност за хардуерна поддръжка на място и замяна на дефектирал компонент

3.3. *Изисквания към изпълнението*

Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или негово официално представителство за правото на разпространение и гаранционна поддръжка на описаните хардуерни продукти на територията на Република България.

4. Поддейност 2.4 „Доставка на нова допълнителна система за съхранение и управление на резервни копия“

5.1.Обхват на услугата

Доставка на специализирано решение за съхранение и управление на резервни копия - 2 броя, съгласно изискванията посочени в Таблица № 17:

Таблица № 17

Минимални изисквания	
REQ.1.	Мрежова карта за връзка с централните точки: - Минимум 4 x 10/25 Gbit/s SFP порта § Минимум 4 x 32Gbit/s SFP порта със съответните SFP+ модули.
REQ.2.	Решението да бъде доставено с минимум 420TB RAW капацитет преди RAID, компресия и дедупликация, с дискове не по-големи от 8TB. Решението трябва да позволява разширение до 840TB
REQ.3.	Всички нужни захранвания да бъдат включени.
REQ.4.	Протоколи за свързаност – решението трябва да поддържа следните протоколи - CIFS , NFS, VTL
REQ.5.	Решението трябва да използва Inline дедупликация и компресия
REQ.6.	Решението трябва да позволява интеграция с бекъп приложения и приложения за данни за дедупликация на данните преди изпращане към хардуерното устройство (client based deduplication)
REQ.7.	Решението трябва да осигурява минимална производителност от минимум 70TB/ч при използването на дедупликация от страна на клиента (client based duduplication)
REQ.8.	Решението трябва да използва блокове с променлив размер за дедупликацията (variable block deduplication)
REQ.9.	Решението трябва да използва глобална дедупликация, без значение

Минимални изисквания	
	на използвания протокол за бекъп (CIFS/NFS/VTL/дедупликация при клиента)
REQ.10.	Решението трябва да предлага валидация на записаните данни
REQ.11.	Решението трябва да предлага криптиране репликация
REQ.12.	Решението трябва да бъде доставено с лицензи за репликация
REQ.13.	Решението трябва да позволява репликация както на всички данни, така и на избрано подмножество (избрана папка, виртуална лента и т.н.)
REQ.14.	Устройството трябва да поддържа моментни копия/snapshots.
REQ.15.	Решението трябва да позволява „заключване" на бекъп информацията (retention lock) за определен период от време
REQ.16.	Решението трябва да позволява репликация със съществуващи системи DD6900 със серийни номера CKM01203620301 и CKM01203620302, без необходимост от външен софтуер и/ или хардуер, освен с необходимия за осъществяване на мрежова свързаност.
REQ.17.	Срок на хардуерната гаранция - минимум 5 (пет) години, в режим 24x7, на място, с предоставяне на обслужване на място в деня на докладването на проблема.
REQ.18.	Срок на техническа поддържка – минимум 5 (пет) години, отдалечено в режим 24x7.
REQ.19.	Получаване на нови версии на софтуера - минимум 5 (пет) години, с включено право да се ползват без допълнително заплащане поправки и нови версии на софтуера за целия срок на поддръжката.

5.2.Параметри на услугата

- Възможност за регистриране на инциденти в сайта на производителя
- Възможност за изтегляне на актуализации от сайта на производителя
- Възможност за хардуерна поддръжка на място и замяна на дефектирал компонент

5.3.Изисквания към изпълнението

Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или негово официално представителство за правото на разпространение/доставка на предлаганите хардуерни продукти на територията на Република България.

5. Поддейност 2.5 „Доставка на нова допълнителна дискова система за обработка и съхранение на данни"

6.1. *Обхват на услугата*

Доставка на нова допълнителна дискова система за обработка и съхранение на данни - 1 брой, съгласно изискванията посочени в Таблица № 18:

Таблица № 18

Позиция	Минимални изисквания
REQ.1.	В дискова система да се предложат минимум 1400 TiB след прилагане на RAID 6 защита в системата и без прилагане на каквито и да е техники за редукция на данните (дедупликация, компресия, тънко провизиране и други).
REQ.2.	За монтаж в стандартен 19“ шкаф, до 4U височина, дълбочина 1000 мм или 1200 мм, с включени всички механични компоненти за коректен монтаж.
REQ.3.	Предложената система трябва да се достави с налични и използваеми поне 48 слота слота/гнезда за устройства за енергонезависимо постоянно съхранение на потребителски данни. Устройствата за съхранение да бъдат SSD/флаш NVMe PCI-Express поколение 4 или 5.
REQ.4.	Предложената дискова система да се достави с минимум една двойка контролери в конфигурация „активен-активен“. Да позволява бъдещо разширение чрез изграждане на мрежа от дискови масиви с мин. 12 контролера (нода).
REQ.5.	Да се достави с минимум 3072 GiB RAM cache за системата. При аварийно спиране на захранването, подлежащите на запис данни в RAM кеш паметта да бъдат съхранени в енергийно независим носител на информация.
REQ.6.	Да се доставят следните портове за връзка със сървъри: минимум по 8 порта на контролер, всеки порт 32 Gbps Fibre Channel (FC). Да поддържа NVMe over FC. Да бъдат включени по 8 броя FC 32 Gbps SW SFP модули на контролер.
REQ.7.	Да се доставят 16 броя оптични кабели, всеки: • с дължина 5 метра; • с LC конектори; • OM3 или OM4.
REQ.8.	Да предоставя резервиране на всички активни компоненти без единична точка за отказ - захранващ модул, контролер, носители на данни.
REQ.9.	Да осигурява замяна на компонент (захранващ модул, батерия, контролер, носител на данни) без прекъсване на достъпа до всички данни.
REQ.10.	Да предоставя възможност за обновление на системния софтуер (firmware) без прекъсване на достъпа до всички данни.
REQ.11.	Пространство за съхранение:
REQ.11.1.	Предложената система за съхранение да се достави с използваемо пространство за съхранение в размер на 1400.00 TiB.
REQ.11.2.	Пространството за съхранение да се постигне с минимум 48 броя еднакви носители на данни SSD/флаш NVMe PCI-Express поколение 4 или 5.
REQ.11.3.	В предложението да се включи документ от официалния инструмент на производителя за оразмеряване на капацитет на съхранение.
REQ.11.4.	Минимум 1 брой от предложените носители на данни да бъде резервно (hot-spare) устройство за съхранение (или повече – ако добрата практика на производителя изисква повече).

Позиция	Минимални изисквания
	Допустимо е вместо посветено резервно (hot-spare) устройство за съхранение на данни, неговото пространство за съхранение да бъде разпределено измежду предложените носители на данни.
REQ.11.5.	Организация на ресурсите на дисковия масив: да се достави с работеща функционалност за изграждане на един общ ресурс за съхранение (т. нар. в индустрията пуул – на англ. pool), включващ всички предложени устройства за съхранение на данни.
REQ.11.6.	Възможности за надграждане на капацитета за съхранение. Предложената конфигурация да позволява надграждане на първоначално доставената конфигурацияс допълнителни SSD/флаш устройства за съхранение с NVMe или SAS интерфейс.
REQ.12.	Предложената система за съхранение да постига минимум 500 000 IOPS (входно-изходни операции в секунда, на англ. IOPS – Input-Output Operations per Second) при времезакъснение, не по-голямо от 0.4 ms и до 55% натоварване на всеки компонент на системата за съхранение при следните характеристики на входно-изходния поток от данни: 1. Fibre Channel протокол за връзка със сървъри. 2. 100% произволен (random) достъп. 3. Четене/запис – 65%/35%. 4. Кеширане при четене: не повече от 25%. 5. Големина на една заявка за четене и запис – 16 KiB. 6. Нула промени на данни в кеша преди запис на данните от кеш към SSD/флаш NVMe носителите на данни. 7. Без: моментни копия, пълни локални копия, отдалечена репликация. 8. Skew = 1. 9. С активна (работеща) за цялото пространство за съхранение поне една от следните функции за редукция на данните – инлайн компресия или инлайн дедупликация. В предложението да се включи документ от официалния инструмент на производителя за оразмеряване на производителност.
REQ.13.	Да включва следните функционалности, лицензирани и използваеми за целия инсталиран капацитет на съхранение на предложения дисков масив и за целия срок на поддръжка: 1. Тънко провизиране (Thin Provisioning). 2. Инлайн дедупликация или инлайн компресия за предложените устройства за съхранение на данни. 3. Моментни копия (Snapshot). 4. Пълни локалния копия (Clones). Да може да се надгради с опционална функционалност за репликиране на данни до поне два публични облака от вида Amazon Web Services, Microsoft Azure, Google Cloud или еквивалент.
REQ.14.	Функции за кибер устойчивост. Предложението да включва лицензирани, активирани и работещи функционалности за:

Позиция	Минимални изисквания
REQ.14.1.	Защитни копия на данните: ○ от вида моментна снимка (снапшот); ○ да не може да се монтират на сървър или ако може да се монтират, да са в режим „само четене“ (read only). ○ изтриването и промяната на копията да е забранено за определени роли потребители, имащи достъп до интерфейсите за управление на дисковия масив. Само точно определени роли администратори на дисковия масив да имат права да изтриват тези копия. ○ копията да се създават автоматично по политика, дефинирана само от определени (високи) роли администратори на масива. Политиката да включва избираеми от потребителя: честота на създаване на копията, времеви период на съхранение на копията, автоматично изтриване на копията след изтичане на периода. ○ ако са необходими допълнителни ресурси (софтуерни продукти/лицензи, хардуерни продукти и други), за изпълнение на тези изисквания, тези ресурси да бъдат включени в предложението и да се опише действието им.
REQ.14.2.	Да има режим за администриране на дисковия масив, при който задължително да се изискват двама администратори за изпълнение на критични задачи.
REQ.14.3.	Пълно криптиране на всички данни на Възложителя при изпълнение на следните условия: • Криптирането да е от вида „в мястото на съхранение“ (т. нар. DaRe – „Data at Rest“). • Да се използва симетрично криптиране на данните с минимум 256-битов ключ. • Ключът за криптиране на самите данни (Media/Data encryption Key = MEK/DEK) да не се съхранява в явен (некриптиран) вид в каквато и да е енергонезависима памет – където и да е. • MEK/DEK (или еквивалент съгласно технологията и терминологията на конкретния производител) да се криптира симетрично с друг (различен) ключ. • В случай, че MEK/DEK се пренася по комуникационен/електронен канал извън физическата кутия на самите NVMe носители на данни, MEK/DEK да бъде криптиран по време и в средата на преноса му до NVMe носителите на данни. • Предложенията да включват решение за управление на криптографските ключове така, че в енергонезависима памет вътре в дисковия масив да не се съхранява информация (ключ и/или друго), която да е достатъчна за успешно декриптиране на данните на Възложителя. • В случай, че изпълнението на горното изискване налага доставка на допълнителни хардуерни и/или софтуерни продукти, те да бъдат включени в предложението и да се опишат.

Позиция	Минимални изисквания
	• Ако се използват външни сървъри за управление на криптографски ключове, да се изгради резервирана сървърна инфраструктура от минимум два такива напълно независими сървъра така, че във всеки момент, частична или пълна загуба на данни, в който и да е от двата сървъра, да позволи успешно декриптиране на всички данни на Възложителя в дисковия масив само с използване на един работещ сървър. В този сценарий, да се предложи и независимо от сървърите решение за пълно декриптиране на всички данни на Възложителя в дисковия масив в случай на пълен срив и пълна загуба на данните във всички сървъри за управление на криптографски ключове. • В случай на използване на сървъри за управление на криптографски ключове, тези сървъри (разбира се) да не използват каквото и да е пространство за съхранение от дисковия масив, чиито криптографски ключове управляват.
REQ.15.	Да се осигурява управление на дисковата система през криптирани графичен интерфейс (GUI) и команден ред (CLI). Графичният интерфейс да показва моментни стойности на натоварването – IOPS и MB/s за четене и запис на хост сървърите; IOPS за бек-енд; времезакъснение.
REQ.16.	Да се достави софтуер за наблюдение на производителността в реално време, лицензиран за цялото предложено пространство за съхранение с включени следните функционалности: • Снемане на отчет през времеви интервал 1 минута или по-малко за поне седем дни. • Мониторинг на производителността на Fibre Channel комутатори Broadcom/Brocade и Cisco – на ниво комутатор и на ниво порт. • Задаване на целеви стойности на избрани метрики за производителност с генериране на известия при неизпълнение на целите. • Планиране на капацитет – софтуерът да притежава аналитични функции за прогнозиране на бъдещи нужди от пространство за съхранение към избрана дата. • Да съхранява информацията за една година назад (допуска се това да бъде с намалена гранулярност на статистическите данни). • Описаните функционалности да се постигнат в локална (необлачна, on-premise) софтуерна среда.
REQ.17.	Да се предостави телеметрична услуга от облачната среда на производителя на дисковия масив. Услугата да включва следните функционалности за отдалечено наблюдение и поддръжка на системата за съхранение: • Графичен потребителски интерфейс (GUI). • Инвентаризация на дисковия масив и отчети за използвания капаците за съхранение. • Мониторинг на капацитет за съхранение – използван, наличен, спестен чрез редукция на данните.

Позиция	Минимални изисквания
	• Запазване на данните за конфигурацията и капацитета за повече от една година. • Бързо изолиране на проблемни събития. • Изпращане на аларми, предсказващи проблеми. • Мониторинг на изправността с функция call home. • Отваряне и управление на заявки за поддръжка (tickets) към производителя. • Събиране и изпращане на журнали (лог файлове) за машината към производителя – от интерфейса на облачната услуга. Всички функционалности да са достъпни през облачно базирания интерфейс на услугата. Ако е необходима сървърна машина за комуникиране на телеметричните данни от дисковия масив към облака, тази машина (с всичките ѝ хардуерни и софтуерни компоненти) да бъде включена в предложението и да се опише.
REQ.18.	С цел постигане на максимална свобода при избор на софтуерни платформи за приложения, дисковият масив да е съвместим с най-масово използваните операционни системи, среди за сървърна виртуализация и среди за управление на контейнерни приложения с утвърдените им популярни версии: Microsoft Windows Server 2022; Red Hat Enterprise Linux® 9.4; CSI драйвър за Red Hat OpenShift 4.18; Ubuntu 22.04, CSI драйвър за Kubernetes 1.32, SUSE Linux Enterprise Server 15 SP6; VMware® vSphere/ESXi 8.0 U3.
REQ.19.	Да се доставят всички необходими крепежни елементи, монтажни комплекти, захранващи кабели, мрежови кабели, оптични кабели както и лицензи, необходими за изпълнение на всички изисквания и за пълноценно функциониране на дисковата система.
REQ.20.	Да се предоставят оригиналните партидни номера на производителя за всички компоненти на предложената конфигурация: • Хардуерни; • Софтуерни; • Поддръжка.
REQ.21.	Конфигурацията да съдържа само оригинално вложени от производителя компоненти. Не се допуска докомплектуване на дисковия масив извън фабриката на производителя.
Гаранция	
REQ.22.	Срок на хардуерната гаранция - минимум 5 (пет) години, в режим 24x7, на място, с предоставяне на обслужване на място в деня на докладването на проблема.
REQ.23.	Срок на техническа поддържка – минимум 5 (пет) години, отдалечено в режим 24x7
REQ.24.	Получаване на нови версии на софтуера - минимум 5 (пет) години, с включено право да се ползват без допълнително заплащане поправки и нови версии на софтуера за целия срок на поддръжката.

6.2. *Параметри на услугата*

- Възможност за регистриране на инциденти в сайта на производителя
- Възможност за изтегляне на актуализации от сайта на производителя
- Възможност за хардуерна поддръжка на място и замяна на дефектирал компонент

6.3. *Допълнителни изисквания*

- Наблюдение на работоспособността на дисковата системата.
- Обучение за работа с дисковата система – до 5 служителя.

6.4. *Изисквания към изпълнението:*

Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или негово официално представителство за правото на разпространение/доставка на предлаганите хардуерни продукти на територията на Република България.

6. Поддейност 2.6 „Доставка на нови сървърни конфигурации“

7.1. Обхват на услугата:

Доставка на нови сървърни конфигурации - 16 броя, съгласно изискванията, посочени в Таблица № 19:

Таблица № 19

Позиция	Параметър / елемент	Описание / минимални изисквания
REQ.1.	**Form factor**	За монтаж в стандартен 19 инчов шкаф с размер максимално 1RU с включени телескопични релси;
REQ.2.	**Процесори**	Два инсталирани процесора;
		Минимум 32 физически ядра;
		Минимум 64 нишки;
		Минимум 2.8 GHz базова работна честота;
		Минимум 60 MB кеш;
		Поддържана памет минимум 6TB;
		Максимално 250W средна топлинна мощност (TPD), при базова работна честота;
		Поддръжка на PCIe Gen4.0;
REQ.3.	**Слотове за памет**	Минимум 32 за целия сървър
		Минимум 16 на 1 брой процесор;
		Слотове за канал минимум два броя;
REQ.4.	**Памет**	Тип DDR5 ECC Registered Капацитет: минимум 1536GB;

		Работна честота: минимум 4800MHz; Възможност за разширение: до минимум 8TB;
REQ.5.	**Вградена графична подсистема**	Тип: Интегрирана;
REQ.6.	**Контролер за външна дискова подсистема**	Един брой FiberCannel (FC) адаптер с двапорта 64 Gbps с включени SFP модули от производителя;
REQ.7.	**Дискова памет за зареждане на ОС или Hypervisor**	Двата носителя: минимум 480 GB конфигурирани в RAID 1
REQ.8.	**Сигурност**	Интегриран на основната платка Discrete Trusted Platform Module 2.0 с TCG сертификация;
REQ.9.	**Контролер за управление**	Контролер за отдалечено управление допускащ CLI режим и уеб TLS графичен режим, възможност за използване на отдалечена медия, пълна KVM функционалност, отделен 1Gbps порт за управление; Конзола за управление, която да поддържа интеграция със: Microsoft System Center, VMware vCenter™, BMC Software Connections: Nagios & Nagios XI, Oracle Enterprise Manager, MicroFocus Operations Manager, IBM Tivoli Netcool/OMNIbus, IBM Tivoli Network Manager, Възможност за внедряване като виртуална машина - ESX, Hyper-V, или Citrix o Съвместима с HTML 5 o Поддръжка на Redfish REST API o Ъпдейти на Firmware/BIOS и проверка за съответствие o Профили за сървърни конфигурации и проверка за съответствие o Разгръщане върху bare metal o Възможност за пълно управление без агент o Възможност за управление на наличната инфрастуктура без нужда от допълнителни лицензи o интеграция с Активна Директория o Възможност за персонализиране на отчети и следене на това дали сървъра е в гаранционна поддръжка или не. o Интеграция с външни мрежи с възможност за call home o Stateless управление, управление на събития и нотификации, базирани на политики
REQ.10.	**Мрежови комуникационни контролери**	Един 1000BaseT Ethernet контролер с 2броя x1Gbps порта;
		Един оптичен мрежови контролер с четири 25Gbps порта с включени 10/25Gbps SFP+ Multimode модула от производителя
REQ.11.	**Захранване**	Тип: Резервирано, вградено в сървъра с възможност за „гореща замяна“ (hot plug);

		Мощност на един захранваш блок: не по-малко от 1000W;
		Platinum клас с ефективност минимум 95%;
REQ.12.	**Интерфейси и портове**	USB 3.0 минимум 1 броя; USB 2.0 минимум 2 броя;
		Минимум един брой аналогов видео изход;
Гаранция		
REQ.13.	Срок на хардуерната гаранция - минимум 5 (пет) години.	
REQ.14.	Срок на техническа поддържка – минимум 5 (пет) години.	
REQ.15.	Получаване на нови версии на софтуера - минимум 5 (пет) години.	

7.2. Параметри на услугата

- Възможност за регистриране на инциденти в сайта на производителя
- Възможност за изтегляне на актуализации от сайта на производителя
- Възможност за хардуерна поддръжка на място и замяна на дефектирал компонент

7.3. Изисквания към изпълнението

Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или негово официално представителство за правото на разпространение/доставка на предлаганите хардуерни продукти на територията на Република България.

IV. Дейност 3: Осигуряване и поддръжка на решения за одит и анализ на промените, решение за управление на привилегирования достъп до отдалечени ресурси (Privileged Access Management – PAM), решение за предотвратяване на загуба на данни и решение за защита и управление на уязвимости, софтуерни лицензи на система за събиране и анализ на логове, осигуряване на хардуерна поддръжка и продължаване правото на ползване и поддръжка за устройства и софтуерни лицензи за защита на Web приложения, осигуряване на нови защитни стени втори слой.

1. Подддейност 3.1: „Подновяване на лицензи за право на ползване и поддръжка за Решение за предотвратяване на загуба на данни (DLP)“

1.12. ***Обхват на услугата***

Настоящата услуга обхваща следните софтуерни лицензи:

- Осигуряване на продължаване правото на ползване и поддръжка на софтуерни лицензи, описани в Таблица 20:

Таблица № 20

Продуктов номер	Описание	Брой	Период на текуща валидност до:	Осигурено право на ползване и поддръжка до:
FDLPSIP	Forcepoint DLP Suite (IP Protection), User & Data Security	9000	28.10.2025г.	31.12.2030г.
SPRT	Enhanced Support	1	28.10.2025г.	31.12.2030г.

1.12. ***Параметри на услугата***

- Възможност за регистриране на инциденти в сайта на производителя
- Възможност за изтегляне на актуализации от сайта на производителя

1.12. ***Изисквания към изпълнението***

Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя на софтуера или от негов официален представител за право на извършване на разпространение на предлаганите софтуерни продукти на територията на Република България.

2. Подддейност 3.2: „Подновяване на лицензи за право на ползване и поддръжка за Решение за защита и управление на уязвимости“

1.12. ***Обхват на услугата***

Настоящата услуга обхваща следните софтуерни лицензи:

- Осигуряване на продължаване правото на ползване и поддръжка на софтуерни лицензи, описани в Таблица 21:

Таблица № 21

Продуктов номер	Описание	Брой	Период на текуща валидност до:	Осигурено право на ползване и поддръжка до:
RNXENTALLTERM	Renewal of Nexpose - Subscription License - Includes Maintenance & Support	9000	28.10.2025г.	31.12.2030г.

1.12. ***Параметри на услугата***

- Възможност за регистриране на инциденти в сайта на производителя
- Възможност за изтегляне на актуализации от сайта на производителя

1.12. ***Изисквания към изпълнението***

Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя на софтуера или от негов официален представител за право на извършване на разпространение на предлаганите софтуерни продукти на територията на Република България.

3. Подддейност 3.3.: Подновяване на лицензи за право на ползване и поддръжка за Решение за одит и анализ на промените

1.12. ***Обхват на услугата:***

Настоящата услуга обхваща следните софтуерни лицензи:

- Осигуряване на продължаване правото на ползване и поддръжка на софтуерни лицензи, описани в Таблица № 22:

Таблица № 22

Код на продукта	Описание	Брой	Валидност на текуща поддръжка до:	Осигурено право на ползване и поддръжка до:
NW-S-NA-AD	Абонамент с включена поддръжка до 31.12.2030г. за Netwrix Auditor for **Active Directory**	9000	28.08.2027	31.12.2030
NW-S-NA-WS	Абонамент с включена поддръжка до 31.12.2030г. за Netwrix Auditor for **Windows Server**	9000	28.08.2027	31.12.2030
NW-S-NA-FS	Абонамент с включена поддръжка до 31.12.2030г. за Netwrix Auditor for **Windows File Servers**	9000	28.08.2027	31.12.2030

Код на продукта	Описание	Брой	Валидност на текуща поддръжка до:	Осигурено право на ползване и поддръжка до:
NW-S-NA-SQL	Абонамент с включена поддръжка до 31.12.2030г. за Netwrix Auditor for **SQL Server**	9000	28.08.2027	31.12.2030
NW-S-NA-VM	Абонамент с включена поддръжка до 31.12.2030г. за Netwrix Auditor for **VMware**	9000	28.08.2027	31.12.2030
NW-S-NA-EX	Абонамент с включена поддръжка до 31.12.2030г. за Netwrix Auditor for **Exchange**	9000	28.08.2027	31.12.2030
NW-S-NA-ND	Абонамент с включена поддръжка до 31.12.2030г. за Netwrix Auditor for **Network Devices** (пакет за 25 мрежови устройства)	20	28.08.2027	31.12.2030

1.12. ***Параметри на услугата***

- Възможност за регистриране на инциденти в сайта на производителя;
- Възможност за изтегляне на актуализации от сайта на производителя.

1.12. ***Изисквания към изпълнението***

Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя на софтуера или от негов официален представител за право на извършване на разпространение на предлаганите софтуерни продукти на територията на Република България.

4. Подддейност 3.4.: Осигуряване на лицензи за право на ползване и поддръжка за Решение за управление на привилегирования достъп до отдалечени ресурси (PAM)

1.12. ***Обхват на услугата:***

Осигуряване на лицензи за право на ползване и поддръжка за Решение за управление на привилегирования достъп до отдалечени ресурси (PAM), съгласно изискванията, посочени в Таблица 23:

Таблица № 23

Позиция	Минимални изисквания
REQ.1.	Предложеното решение трябва да включва технология за управление на привилегирования достъп до отдалечени ресурси (PAM), абонамент с включена поддръжка до 31.12.2030г. за 300 привилегировани акаунти.
REQ.2.	Да може да сканира непрекъснато за неуправлявани или непознати привилегировани акаунти, за премахване на излишен достъп до ресурси.
REQ.3.	Да се използва технология с презумция без доверие към привилегированите потребители (zero-trust), като решението да може да предоставя само необходимия достъп на оторизираните лица за необходимото им време, премахвайки излишните привилегии след завършване на отдалечените сесии (just-in-time технология), като самите сесии да се записват във видеоформат в реално време и да се съхраняват с всичките им метаданни и изпълнени действия за целите на одитириане и търсене в тях.
REQ.4.	Да се предоставя през решението само необходимият достъп на потребителите, да не се използват локални администраторски акаунти.
REQ.5.	Да може да се предоставя временен администраторски достъп до ресурс, с пълен запис на сесията, като автоматично да се премахва достъпа след завършване на сесията за отдалечен достъп.
REQ.6.	Да може да се предоставя достъп до ресурси от централизираната конзола на решението без да е необходимо да се споделят права за достъп до ресурсите с привилегированите потребители, да могат да са маскирани за тях.
REQ.7.	Да може да се предоставя достъп за изпълнение само на определени привилегировани команди по време на отдалечени сесии, като самите команди да се одитират и логират.
REQ.8.	Да се предоставя визуализация на взаимовръзките в средата на организацията като да могат да се мониторират и управляват всички акаунти и всяка активност от тях.
REQ.9.	Да може да се ограничи какъв софтуер може да се инсталира от привилегированите потребители, да може да се управлява работата им с преносими устройства за съхранение на данни по време на привилегированите сесии, както и да могат да се управляват промени по конфигурациите на наличните приложения на крайните точки.
REQ.10.	Да може да се валидира, че настройките по Груповите политики са наложени коректно в средата.
REQ.11.	Да може да се управлява привилегированият достъп до локални, облачни и хибридни ресурси от едно решение.
REQ.12.	Да могат всички действия по управление, предоставяне и премахване на временен just-in-time привилегирован достъп и одитиране и запис на сесии с привилегирован достъп да се извършват автоматично по предварително зададени правила.
REQ.13.	Да има включена клиентска част за привилегированите потребители, където те да виждат и да могат лесно с един клик да достъпят само ресурсите, до които би трябвало да имат достъп, като стартирането на сесиите и налагането на правилата за сигурност в тях да става автоматично от решението, прозрачно за потребителите.
REQ.14.	Решението да може да се поставя на Windows Server 2022, директно или във виртуална среда от тип VMware ESX/ESXi 4.0.

Позиция	Минимални изисквания
REQ.15.	Клиентската част на решението да може да се достъпва през уеб-браузър, минимално Microsoft Edge, Google Chrome, Apple Safari и Mozilla Firefox.
REQ.16.	Решението да може да се интегрира и да управлява привилегирования достъп до Активна директория, Windows работни станции и сървъри, бази от данни тип SQL и Oracle, Microsoft Entra ID, Cisco IOS мрежови устройства, Linux сървъри с различни дистрибуции, използващи SSHv2 (Debian, CentOS, RHEL, openSUSE).
REQ.17.	Решението да може да се интегрира и да управлява привилегирования достъп с поне лимитирани функции до всяко устройство с SSH достъп и до всяка платформа, която се автентикира през Активна директория или през Microsoft Entra ID.
REQ.18.	Решението да може да управлява пароли самостоятелно или да може да се интегрира чрез Rest API до хранилища за пароли от трети страни.
REQ.19.	Решението да може да се интегрира с решения от трети страни за управление на локални администраторски пароли, опростявайки процеси, извършвайки промените по паролите директно от Активна директория.
REQ.20.	Решението да може да се интегрира с основното решение за одит на промените на производителя, за целите на детайлен одит на привилегирования достъп и идентифициране на потенциални рискове.
REQ.21.	Решението да поддържа използването на мулти-факторна автентикация на привилегированите потребители.
REQ.22.	Срок на софтуерна поддръжка - до 31.12.2030г.
REQ.23.	Срок на техническа поддържка – до 31.12.2030г.
REQ.24.	Получаване на нови версии на софтуера - до 31.12.2030г., с включено право да се ползват без допълнително заплащане поправки и нови версии на софтуера за целия срок на поддръжката.

1.12. ***Параметри на услугата***

- Възможност за регистриране на инциденти в сайта на производителя
- Възможност за изтегляне на актуализации от сайта на производителя

1.12. ***Изисквания към изпълнението***

Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя на софтуера или от негов официален представител за право на извършване на разпространение на предлаганите софтуерни продукти на територията на Република България.

5. Подддейност 3.5.: Осигуряване на нови защитни стени втори слой – 2 броя

1.12. ***Обхват на услугата***

Осигуряване на нови защитни стени втори слой, съгласно изискванията, посочени в Таблица 24:

Таблица № 24

Позиция	Минимални изисквания
REQ.1.	Минимална пропускателна способност с активирана функция за идентификация на приложенията - 18 Gbps.
REQ.2.	Минимална пропускателна способност с активирани всички функционалности за защита: IPS/ AntiVirus/AntiMalware/URL/Firewall/Application Control – 10 Gbps.
REQ.3.	Минимална производителност за IPsec VPN – 9 Gbps.
REQ.4.	Минимален брой сесии - 2 200 000.
REQ.5.	Минимален брой нови сесии в секунда - 220 000.
REQ.6.	Разпознати и поддържани приложения – минимум 5 000 броя.
REQ.7.	Минимален брой мрежови интерфейси: • Да разполага с 12x1/2.5/5/10G Base-T ports; • Да разполага с 10x1/10G SFP/SFP+ интерфейса; • Да има възможност за допълнителни минимум 4x25G SFP28.
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) - 1000 SSL VPN потребителя.
REQ.12.	Минимален брой IPSec Site-to-Site VPN - 2000 отдалечени точки.
REQ.13.	Устройството да поддържа виртуални таблици за маршрутизация минимум 11 броя.
REQ.14.	Устройството да има възможност да поддържа виртуализация (виртуални контексти) – 11 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): • 1 x 10/100/1000 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).
Функционални изисквания към системата	
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.
REQ.26.	Предлаганата защитна стена трябва да може да изпраща минимум 2000 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 чрез 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.	Предложеното решение трябва да 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 през неговия графичен интерфейс, без да е 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 ВЪЗЛОЖИТЕЛЯ 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 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.
Гаранция, поддръжка и лицензи:	
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.

6. Подддейност 3.6.: Осигуряване на хардуерна поддръжка и продължаване правото на ползване и поддръжка за устройства и софтуерни лицензи за защита на Web приложения.

1.12. *Обхват на услугата*

Осигуряване на хардуерна поддръжка и продължаване правото на ползване и поддръжка на софтуерни лицензи за следните видове продукти описани в Таблица 25:

Таблица № 25

№	Вид техника	Сериен номер	Брой	Период на текуща валидност до:	Период на валидност до:
REQ.1.	F5-BIG-LTM-I5800	f5-fdno-bkid	1	28.10.2025г.	31.12.2030г.
REQ.2.	F5-ADD-BIG-GBT-I58XX	f5-fdno-bkid	1	28.10.2025г.	31.12.2030г.
REQ.3.	F5-BIG-LTM-I5800	f5-inys-zvdd	1	28.10.2025г.	31.12.2030г.
REQ.4.	F5-ADD-BIG-GBT-I58XX	f5-inys-zvdd	1	28.10.2025г.	31.12.2030г.

№	Вид техника	Сериен номер	Брой	Период на текуща валидност до:	Период на валидност до:
REQ.5.	F5-SBS-BIG-IPI-5-3YR	f5-fdno-bkid	1	28.10.2025г.	31.12.2030г.
REQ.6.	F5-SBS-BIG-IPI-5-3YR	f5-inys-zvdd	1	28.10.2025г.	31.12.2030г.
REQ.7.	F5-SBS-BIG-IPI-5-1YR	f5-fdno-bkid	2	28.10.2025г.	31.12.2030г.
REQ.8.	F5-SBS-BIG-IPI-5-1YR	f5-inys-zvdd	2	28.10.2025г.	31.12.2030г.

Параметри на услугата

- Възможност за регистриране на инциденти в сайта на производителя;
- Възможност за изтегляне на актуализации от сайта на производителя;
- Възможност за подмяна на дефектирало устройство най-късно до края на следващ работен ден.

Изисквания към изпълнението

Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или официален негов представител за право на разпространение на предлаганите продукти и услуги на територията на Република България.

7. Поддейност 3.7 „Подновяване на софтуерна поддръжката на система за събиране и анализ на логове - IBM Qradar SIEM “

Обхват на услугата

Подновяване на софтуерна поддръжката на система за събиране и анализ на логове - IBM Qradar SIEM, описани в Таблица № 26:

Таблица № 26

Наименование	Количество	Валидност на текуща поддръжка до:	Осигуряване на поддръжка до:
IBM Security QRadar Software Install Annual SW Subscription & Support Renewal 12 Months	1	30.11.2025г.	31.12.2028г.
IBM Security QRadar Event Capacity 2.5K Events Per Second Annual SW Subscription & Support Renewal 12 Months	6	30.11.2025г.	31.12.2028г.
IBM Security QRadar Flows Capacity 10K Flows Per Minute Annual SW Subscription & Support Renewal 12 Months	5	30.11.2025г.	31.12.2028г.

Наименование	Количество	Валидност на текуща поддръжка до:	Осигуряване на поддръжка до:
IBM Security QRadar Data Store Connection Annual SW Subscription & Support Renewal 12 Months	1	30.11.2025г.	31.12.2028г.
IBM Security QRadar Software Node Install License + SW Subscription & Support 12 Months	1		31.12.2028г.

Параметри на услугата

- Да се осигури следното ниво на поддръжка за периода до 31.12.2028г.:
- Актуализиране на продукти;
- Обновяване продукти, сигнатури и дефиниции;
- Поддръжка по електронна поща;
- Отваряне на неограничен брой казуси към производителя.

Изисквания към изпълнението

Изпълнителят следва да осигури лиценза от лице, надлежно оторизирано от производителя на софтуера или от негов официален представител за предоставено право на извършване на разпространение на предлаганите софтуерни продукти на територията на Република България.

V. Дейност 4: Осигуряване на решение за защита на крайни потребители, e-mail среда, мрежова инфраструктура.

1. Обхват на услугата

Осигуряване на лицензи за право на ползване и поддръжка и доставка на хардуерни устройства съгласно минималните технически описания, както следва:

1.1. Решение за защита на крайни потребители и сървъри

Таблица № 27

Позиция	Минимални изисквания -
REQ.1.	Брой на крайните точки: **9000**
REQ.2.	Тип решение: Подновяване и обновяване на **Trellix Endpoint Security**, включващо: **1 брой основно хардуерно устройство Trellix Endpoint Detection & Response appliance с вграден софтуер и включена поддръжка до 31.12.2030г.; 1 брой Trellix хардуерно устройство за DMZ с вграден софтуер и включена поддръжка до 31.12.2030г.; абонамент до 31.12.2030г. за 9000 лицензи (софтуерни агенти) Trellix Advanced Endpoint Security** за поставяне на крайните точки, с включена поддръжка **до 31.12.2030г.**
REQ.3.	Решението да предоставя цялостна защита за крайни точки, включително засичане и превенция на атаки, да предоставя функции за разследване и почистване (в зависимост от метода на имплементация на решението), като да се поддържат минимално следните операционни системи на крайните точки: Windows 7, Server 2008), mac OS X и Linux (RHEL, CentOS, Ubuntu, Suse).
REQ.4.	Решението трябва да включва специализирано устройство (хардуер), което да служи за централизирано управление на инсталираните агенти по крайните точки, за да могат да се наблюдават всички защитени крайни точки за съмнително зловредно поведение и да може да се извършва централизирано разследване.
REQ.5.	Агентите на решението трябва да могат да засичат, анализират и позволяват ответна реакция на напреднали кибератаки, използващи непознати „zero-day" уязвимости, независимо дали крайните точки се намират във или извън мрежата на организацията.
REQ.6.	Комуникацията между софтуерните агенти и централизираното управление трябва да е криптирана.
REQ.7.	Агентите на крайните точки трябва да са с малък размер, с минимално влияние на производителността на системите, като да се предоставя механизъм за контролиране на какъв процент от процесорната мощ на крайните точки да се използва за анализ и превенция на атаки, така че да не се влияе на нормалната работа на потребителите.
REQ.8.	Решението трябва да предоставя минимално следните функционалности: • Корелация в реално време на индикаторите за компроментиране на ниво крайна точка. • Засичане и блокиране на exploit атаки, използвайки алгоритми за анализиране на поведението на приложенията. Засичане на ROP

Позиция	Минимални изисквания -
	(Return Oriented Programming) атаки, reverse shell, heap spray, SEHOP corruption, атаки използващи Java уязвимости. • Засичане на зловредни файлове в реално време. • Сканиране на файлове, използвайки антивирусни алгоритми с дефиниции и чрез евристичен анализ. • Сканиране на изпълними файлове чрез алгоритми за машинно обучение (machine learning). • Възможност за сортиране на информация, за да може да се потвърди наличието на дадена атака и за да може да се възпроизведе целия ѝ жизнен цикъл за анализ. • Автоматично създаване на графика с хронолигично подредени събития, довели до компроментирането на дадена крайна точка. • Възможност за изключително бързо търсене в избрани крайни точки за зададени ключови думи, MD5 / SHA1 и SHA256 суми, сложни изрази, създадени файлове в зададен интервал от време, конкретни „бисквитки“, име на DNS хост, конкретни драйвери, файлови атрибути, HTTP хедъри, IP адреси, използвани портове за мрежова комуникация и активни процеси, конкретни ключове в регистрите на операционната система, Windows събития. • Функцията за търсене на информация трябва да може да се използва директно от графичния интерфейс на решението, както и използвайки API интерфейс, така че да могат да се използват автоматизирани скриптове. • Да могат да се изолират заразените крайни точки директно от централизираното управление на решението (по заявка от администратор), позволявайки им комуникация само с посочени IP адреси (Endpoint containment).
REQ.9.	Решението трябва да може автоматично да събира и да предоставя информация за използвани уязвимости, процеси, домейни, регистри, файлове и мрежова активност за вдигнатите аларми. Информацията трябва да е достъпна за преглед директно от графичния интерфейс на конзолата за централизирано управление.
REQ.10.	Решението трябва да позволява извличането на файлове от системите, на които има инсталиран агент. За Windows операционни системи, решението трябва да може да извлича заключени или изтрити файлове, ако те все още не са презаписани от нова информация.
REQ.11.	Решението трябва да позволява извличането на файлове, които са записани на крайните точки в следствие на зловредна активност, директно от интерфейса за разследване на аларми на централизираното управление.
REQ.12.	Функцията за извличане на файлове трябва да може да се използва директно от графичния интерфейс на решението, както и използвайки API интерфейс, така че да могат да се използват автоматизирани скриптове.
REQ.13.	Решението трябва да може автоматично да генерира пакети с данни от крайните точки (endpoint triage), за да се подпомогне разследването на аларми. Пакетите с данни трябва да съдържат информация за системните

Позиция	Минимални изисквания -
	параметри на крайната точка, процесите, файловете, регистрите, потребителските акаунти, история на браузването.
REQ.14.	Решението трябва да позволява извличането на информация за подпомагане на разследванията, като историята на извиканите shell команди, цялото дисково пространство на дадена крайна точка, цялата информация от паметта на крайната точка, историята на извиканите powershell команди, списък на процесите в паметта, списък на файловете на дисковото пространство на крайната точка.
REQ.15.	Решението трябва да може да получава индикатори за компроментиране директно от производителя и от другите подсистеми за киберсигурност, както и да се позволява създаването на собствени индикатори за компроментиране от администраторите, също така да е възможна и интеграцията с външни източници на индикатори.
REQ.16.	Решението трябва да позволява наблюдението на крайни точки и засичане на вируси тип троянски кон, червеи, шпионски софтуер, adware, key logger вируси, rootkit вируси и exploit вируси, които се появяват след употребата на приложения като например Adobe Reader, Adobe Flash, Internet Explorer, Firefox, Google Chrome, Java, Microsoft Outlook, Microsoft Word, Microsoft Excel и Microsoft PowerPoint, включително да могат да се блокират и спират от агента заразените приложения.
REQ.17.	Решението трябва да може да изпраща файлове за по-нататъшен анализ към подсистема за sandbox анализ, разположена локално в структурите на организацията (on premise).
REQ.18.	Решението трябва да може да следи изпълнението на файлове, като да може да определи, дали са изпълнени за първи път или пътят на изпълнение на файловете е променен. Тази информация (мета данни) трябва да може да се изпраща към решение тип SIEM чрез интеграция.
REQ.19.	Решението трябва да може да засича непознати „zero-day" атаки, като динамичният анализ на поведението на процесите трябва да работи минимално за .dll, .ocx, .sys и изпълними (.exe) файлове, като анализът се извършва локално, без да е необходимо изпращането на проби към облачни услуги или трети OEM решения.
REQ.20.	Агентите на решението трябва да могат да записват локално събитията, свързани с работата с файлове (създаване, отваряне, модифициране), с мрежовите комуникации от крайните точки, DNS заявките, достъпените URL адреси, стартираните процеси, с използваните ключове от регистрите на операционната система.
REQ.21.	Решението трябва да позволява да се изолират заразените крайни точки директно от централизираното управление на решението (по заявка от администратор), позволявайки им комуникация само с посочени IP адреси (Endpoint containment), така че да се спре разпространението на заразата по мрежата. Механизмът трябва да позволява използването на различни роли на потребителите, които да правят заявки за изолиране на заразена крайна точка и които да одобряват заявките.
REQ.22.	Решението трябва да може централизирано да обновява софтуерната версия на инсталираните агенти.

Позиция	Минимални изисквания -
REQ.23.	Решението трябва да разполага с механизми за собствена защита от спиране или рестартиране на инсталираните агенти, както и от инжектиране на нежелани процеси в тях.
REQ.24.	Решението трябва да предоставя механизъм с използване на парола, за да се предотврати премахването на инсталиран агент от неоторизирано лице.
REQ.25.	Решението трябва да разполага с добре описан API интерфейс за интегриране.
REQ.26.	Решението трябва да позволява администрация чрез уеб-базирана конзола, без да се изисква инсталирането на допълнителен софтуер за достъпването ѝ.
REQ.27.	Решението трябва да позволява използването на прокси с оторизация за свързване със сървър за обновления на софтуера и информацията за нови заплахи.
REQ.28.	Решението трябва да може да създава, съхранява и предоставя log файлове към трети решения, използвайки Syslog протокол, например за предоставяне на информация на решения от тип SIEM.
REQ.29.	Решението трябва да позволява интеграция с решения тип SIEM за автоматична подмяна на заявки и информация, така че да се намали необходимото време за разследване на атака.
REQ.30.	В случаите, когато агентът не може да установи комуникация с устройството-контролер, агентът трябва да продължи нормалната си работа и да изпрати събраната информация към контролера, когато комуникацията се установи отново.
REQ.31.	Решението трябва да може да се интегрира с решението за защита за e-mail среда от напреднали атаки за корелация на събития през решението за централизирано управление.
Софтуерна поддръжка от производителя	
REQ.32.	Срок: **до 31.12.2030г.**
REQ.33.	Тип поддръжка: 24x7x365
REQ.34.	Възможност за обновление на софтуера в периода на поддръжката
REQ.35.	Възможност за обновления на информацията за заплахите от базата данни на производителя

Таблица № 28

Позиция	**Изисквания към 1 брой основно хардуерно устройство Trellix Endpoint Detection & Response appliance с вграден софтуер и 1 брой Trellix хардуерно устройство за DMZ с вграден софтуер**
REQ.36.	Всяко от устройствата да може да управлява сигурността на до 100 000 крайни точки (максимален капацитет на скалируемост)
REQ.37.	Всяко от устройствата да е с максимална големина 1U
REQ.38.	Всяко от устройствата да разполага с ефективно място за съхранение на получените данни от крайните точки, минимално 8TB
REQ.39.	Всяко от устройствата да работи в изолиран режим, без Интернет свързаност. Всяко от устройствата да не изпраща данни към производителя за засечените заплахи в организацията.

Позиция	Изисквания към 1 брой основно хардуерно устройство Trellix Endpoint Detection & Response appliance с вграден софтуер и 1 брой Trellix хардуерно устройство за DMZ с вграден софтуер
REQ.40.	**Гаранция**
REQ.41.	Срок: **до 31.12.2030г.**
REQ.42.	Тип поддръжка: 24x7x365 (възможност за хардуерна подмяна при дефектирало устройство)
REQ.43.	Възможност за обновление на firmware-а на всяко от хардуерните устройства

1.2. Решение за защита за e-mail среда от напреднали атаки

Таблица № 29

Позиция	Минимални изисквания
REQ.44.	Брой потребители: 9000
REQ.45.	Тип решение: Подновяване и обновяване на **Trellix Email Security**, включващо: **2 броя хардуерни устройства Trellix Email Security (High-Availability)** с вграден софтуер и включена поддръжка **до 31.12.2030г.**, както и включен **абонамент до 31.12.2030г. Trellix Email Security за 9000 потребителя** , с включена поддръжка **до 31.12.2030г.**
REQ.46.	Решението трябва да може да открива и идентифицира зловреден код, който е скрит и влиза в организацията чрез електронната поща, като трябва да се използват технологии и методи за засичане, които да не са базирани само на статичен анализ чрез дефиниции, статични списъци или правила, а да може да извършва и динамичен анализ и да открива непознати "zero-day" заплахи.
REQ.47.	Решението трябва да се предоставя под формата на специализиран хардуер, като производителят трябва да предостави лицензи за софтуер за поне 120 виртуални машини за анализ, с прилежащите им операционни системи и приложения.
REQ.48.	Решението трябва да може да открива фишинг и spear-фишинг атаки. Трябва да може да анализира прикачени файлове и URL адреси в електронните съобщения, за да открива опити за компроментиране на системите на организацията.
REQ.49.	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.50.	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.51.	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.

Позиция	Минимални изисквания
REQ.52.	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.53.	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.54.	Решението трябва да може да извлича и анализира вмъкнати файлове в документи, като например pdf, rtf или MS Office документи.
REQ.55.	Решението трябва да може да поставя в карантина и да алармира за криптирани MS Office документи.
REQ.56.	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.57.	Решението трябва да може да поставя в карантина и да алармира за електронни съобщения, които съдържат в себе си съкратени URL адреси.
REQ.58.	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.59.	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.60.	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.61.	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.62.	Решението трябва да може да анализира URL адреси от тип ftp, http и https.
REQ.63.	Решението трябва да може да анализира base64 кодирани URL адреси.
REQ.64.	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.65.	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).

Позиция	Минимални изисквания
REQ.66.	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.67.	Решението трябва да може да анализира (във виртуалните машини за динамичен анализ) сваленитe файлове от заявки, идващи от exploit атаки. Например, ако прикачен файл към електронно съобщение съдържа скрипт / макрос, който опитва да свали допълнителни файлове и съдържание, то решението трябва да може успешно да ги свали и анализира, за да се открият и предотвратят атаки, които се развиват на няколко фази.
REQ.68.	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.69.	По време на анализа във виртуалните машини, решението трябва да може да извлича и анализира URL адресите в паметта на машините.
REQ.70.	Решението трябва да може да засича ransomware криптиращи атаки и атаки, предназначени за POS терминали.
REQ.71.	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.72.	Решението трябва да предоставя цялостна информация след анализ на зловреден код. Информацията трябва да включва използвани уеб линкове за атаката, хеш суми на сваленитe файлове, цялостен одит на действията по системите (променени ключове от регистрите, създаване и изпълнение на файлове, промяна в автоматичните настройки и параметрите за стартиране на приложения), както и да се предоставя информация за хронолигчния ред от събития, свързани с атаката, започващи от фазата на уеб-експлоатация и първоначално проникване, до свалянето на код, установяване на контрол над системите и опитите за извличане на данни извън организацията.
REQ.73.	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.74.	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.75.	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.76.	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.

Позиция	Минимални изисквания
REQ.77.	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.78.	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.79.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н. Решението трябва да използва собствен, специално изграден хипервайзор.
REQ.80.	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.81.	Решението трябва да може да засича опити за използване на функциите за приспиване (sleep) на операционните системи от зловредния код и да може да забързва времето на виртуалните машини за анализ, за да принуди изпълнението на зловредния код.
REQ.82.	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.83.	Email решението трябва да поддържа inline MTA режим на работа.
REQ.84.	Email решението трябва да поддържа SPAN/TAP режим на работа.
REQ.85.	Email решението трябва да поддържа BCC режим на работа.
REQ.86.	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.87.	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 артефакти, които са му необходими, за да се изпълни изцяло за анализ.
REQ.88.	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.89.	Цялостният анализ на електронното съобщение не трябва да отнема повече от 10 минути.

Позиция	Минимални изисквания
REQ.90.	Решението трябва да позволява на администраторите да конфигурират максималното време за анализ на електронните съобщения.
REQ.91.	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.92.	Решението трябва да може да засича и отчита опити за мрежова комуникация с Интернет от виртуалните машини по време на анализа.
REQ.93.	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.94.	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.95.	Решението трябва да може да работи в напълно изолирана среда, без връзка с Интернет.
REQ.96.	Решението трябва да може да изпраща автоматични известия чрез Syslog, HTTP, SNMP и SMTP протоколи.
REQ.97.	Решението трябва да поддържа криптирана TLS комуникация (opportunistic или imposed), за да се запази конфиденциалността на електронните съобщения.
REQ.98.	Решението трябва да може да изпраща автоматични известия, когато блокира или постави в карантина дадено електронно email съобщение.
REQ.99.	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.100.	Решението трябва да позволява използването на прокси с оторизация за свързване със сървър за обновления на софтуера и информацията за нови заплахи.
REQ.101.	Решението трябва да позволява администрация чрез уеб-базирана конзола, без да се изисква инсталирането на допълнителен софтуер за достъпването ѝ.
REQ.102.	Решението трябва да позволява конфигурирането на ACL списъци, за да се ограничи достъпа до интерфейса за централизирано управление.
REQ.103.	Решението трябва да използва криптирана комуникация между администраторите и конзолата за централизирано управление. Трябва да позволява вмъкването на собствени дигитални сертификати на организацията.
REQ.104.	Решението трябва да позволява локално конфигуриране или чрез синхронизация с NTP сървър на използваните време и часова зона.
REQ.105.	Решението трябва да поддържа ролево-базиран достъп до конзолата за управление. Да могат да се задават различни профили и права (администратор, оператор, одитор и т.н.), като да задават кои отчети, аларми и информация могат да виждат в конзолата за управление.
REQ.106.	Решението трябва да поддържа LDAP, TACACS + или RADIUS методи за вписване на потребителите.
REQ.107.	Решението трябва да може да изпраща известия за собственото си здраве и процеси и генерираните отчети, чрез SMTP, SNMP и Syslog протоколи.

Позиция	Минимални изисквания
REQ.108.	Решението трябва да позволява извличането на аларми и отчети за активност на зловреден код в PDF формат.
REQ.109.	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.110.	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.111.	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.112.	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.
Софтуерна поддръжка от производителя	
REQ.113.	Срок: **до 31.12.2030г.**
REQ.114.	Тип поддръжка: 24x7x365
REQ.115.	Възможност за обновление на софтуера в периода на поддръжката
REQ.116.	Възможност за обновления на информацията за заплахите от базата данни на производителя

Таблица № 30

Позиция	Изисквания към 2-та броя хардуерни устройства Trellix Email Security (High-Availability) с вграден софтуер
REQ.117.	Устройството да може да анализира поне 3000 уникални прикачени файлове към email съобщения в час
REQ.118.	Устройството да може да анализира прикачени файлове и URL адреси в email съобщенията за 9000 пощенски кутии
REQ.119.	Устройството да е с максимална големина 2RU
REQ.120.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
REQ.121.	**Гаранция**
REQ.122.	Срок: **до 31.12.2030г.**
REQ.123.	Тип поддръжка: 24x7x365 (възможност за хардуерна подмяна при дефектирало устройство)
REQ.124.	Възможност за обновление на firmware-а на хардуерното устройство

1.3. Решение за защита на мрежовата среда от напреднали атаки

Таблица № 31

Позиция	Минимални изисквания
REQ.1.	Тип решение: Подновяване и обновяване на **2 броя хардуерни устройства Trellix Web Security appliance (High-Availability)** с вграден софтуер и включена поддръжка **до 31.12.2030г.**
REQ.2.	Предложеното решение трябва да може да инспектира и блокира зловреден мрежови трафик като да се поставя на пътя на трафика в inline режим или в „out-of-band“ режим, трябва да може да работи независимо от останалото мрежово оборудване в инфраструктурата.
REQ.3.	Решението да поддържа режим на работа с висока достъпност - high availability (HA), от типа active-active.
REQ.4.	Решението трябва да може да функционира независимо от което и да е друго мрежово устройство (например защитни стени, IDS/IPS устройства, security gateway устройства и т.н.). Решението трябва да е специализирано и да може да работи самостоятелно, като функциите му не трябва да са част от UTM или интегрирано решение за сигурност.
REQ.5.	Предложеното решение трябва да предоставя предварително зададени правила за разпознаване на зловредни мрежови действия от приложенията, разположени по работните станции и сървърите в инфраструктурата на организацията. Трябва да има възможност за обновяване на тези правила, използвайки актуална информация, събрана от вендора за най-новите заплахи.
REQ.6.	Решението трябва да може да анализира мрежови трафик от организацията към Интернет и да засича изпълнението на нежелани приложения или callback комуникации с хакерски командни центрове, като по тази начин да могат да се блокират опити за изнасяне на информация извън организацията по мрежата, като или се блокира мрежовата сесия, ако се работи в inline режим или като се вграждат „reset“ пакети в комуникацията, ако се работи в „out-of-band“ режим.
REQ.7.	Решението да може да функционира като ICAP сървър, като трябва да може да получава файлове за анализ чрез ICAP протокола.
REQ.8.	Решението трябва да може да засича ранните фази на уеб-базираните атаки, например първоначално стартиране на exploit, сваляне на зловреден бинарен код, callback функции и комуникации с хакерски командни центрове, за да може да идентифицира уязвимости в системите и приложенията на организацията, за да може да засича заразени системи и за да може да блокира неоторизирани комуникации навън от средата, по няколко мрежови протокола.
REQ.9.	Предложеното решение трябва да може да инспектира и да открива зловредни обекти, зловредни URL мрежови адреси и зловредни действия в поне следните мрежови протоколи: HTTP, HTTPS, FTP, SMB.
REQ.10.	Предложеното решение трябва да може да засича движение на атаките „настрани“ в организацията (lateral spread) като анализира SMB, WinRM и MS-SQL трафик и да може да засича и алармира за дейности след успешен exploit на уязвимости от атакуващите, от вътрешна работна станция до вътрешен трафик (трафик тип изток-запад), като например

Позиция	Минимални изисквания
	вътрешно разузнаване, ескалиране на права за достъп на акаунти, извличане на потребителски имена и пароли, движение „настрани“ на зловреден код, изпълнение на дистанционни команди, извличане на данни.
REQ.11.	Предложеното решение трябва да е под формата на специализирано хардуерно устройство, като производителят трябва да предостави пълни лицензи за софтуера, който ще се използва от устройството за анализиране на зловреден код, както и необходимите лицензи за операционните системи и приложенията, използвани от виртуалната среда за анализ на кода.
REQ.12.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението трябва да използва собствен, специално изграден хипервайзор.
REQ.13.	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.14.	Решението трябва да предоставя среда за динамичен анализ, която да се състои от предварително създадени виртуални машини, които да са изцяло предоставени и поддържани от вендора на решението, за да се избегне сложността произтичаща от инсталирането на приложения и поддръжката на виртуални машини от страна на организацията.
REQ.15.	Решението трябва да може да идентифицира атаки, без да внася забавяне в мрежовия трафик на организацията, като анализът трябва да се извършва локално, на мрежовото ниво, където е разположено устройството.
REQ.16.	Решението трябва да има механизъм за класифициране и поставяне на етикети на бинарен код на машинно ниво, които се отнася за EXE, DLL и SYS файлове.
REQ.17.	Предложеното решение трябва да дава възможно най-малко грешни показания и да вдига възможно най-малко грешни аларми при засичането на файлове, които наподобяват зловреден код: да алармира за поведение, което опитва да избегне засичане от системите за сигурност, инсталиране на нежелани програми, промяна на системните настройки, което влошава производителността на системите, наличие на потенциално нежелани програми (PUP) и на потенциално нежелани приложения (PUA), adware процеси и използване на инструменти, които често се използват от атакуващи хакери.
REQ.18.	Решението трябва да може да разпознава заплахи чрез извършване на локален анализ, без да се изпращат файлове, проби от кода или изпълним код извън организацията или към облачно-базирани системи за анализ.

Позиция	Минимални изисквания
REQ.19.	Трябва да има възможност за комплексно разследване за целия цикъл на атаките, включително върху всяка от следните фази, за които да има отделни аларми: • Първоначално разпознаване на мрежата (Картографиране на мрежата, преброяване на хостовете, преброяване на услугите, издирване на потребителски акаунти); • Изпълнение (използване на командата „AT“ за насрочване на изпълнение на процеси, „pass-the-hash“ дистанционно изпълнение на код (RCE), използване на инструментариума за управление на Windows средите (WMI), дистанционно създаване на процеси); • Изпълнение на Web Shell; • Сваляне на зловреден код (malware); • Извличане на информация чрез свързвания с хакерски команден сървър; • Разпространяване на зловредния код (трансфер на зловреден код чрез SMB и SMB 2 протоколи) • Ескалиране на привилегии (преброяване на групите с високо ниво на достъп, преброяване на дистанционно споделените ресурси - remote shares) • Извличане на данни за вписване в системите (трансфер на пароли чрез SMB протокол, извличане чрез Mimikatz, извличане на NTLM хешове) • Дистанционно изпълнение на процеси.
REQ.20.	Решението трябва да може да идентифицира уеб-базирани уязвимости, чрез извършване на анализ на съмнително уеб съдържание във виртуалните машини за анализ, използвайки същия тип браузър, както реалният потребител, достъпил уеб съдържанието.
REQ.21.	Решението трябва да може да засича атаки към сървърите като извлича и анализира статични и динамични уеб-базирани файлове (PHP, WAR, JSP, ASP, ASPX), които са качени на уеб сървърите чрез HTTP POST или FTP.
REQ.22.	Решението трябва да предоставя детайлна информация за аларми, произлизащи от извлечените метаданни от транспортния и от приложния слой на мрежата, за поне следните протоколи: FTP, HTTP, IMAP, IRC, POP3, RDP, RTSP, SIP, SMB, SMTP, SSH, TLS; Решението трябва да може да визуализира метаданните в интерактивна, графична форма, както и да позволява извличането им за интегриране с трети SIEM решения.
REQ.23.	Решението трябва да може да инспектира HTTPS трафик, като да се поддържат SSL / TLS протоколи, включително да се поддържат функции като JA3 fingerprinting, използване на „бели списъци“ и URL категоризация.
REQ.24.	Решението трябва да може да анализира поне следните файлови типове: msi, exe, dll, pdf, doc, chm, avi, jar, docx, xls, xlsx, gif, jpeg, png, tiff, swf, swf embedded in swf, scr, mov, qt, mp4, jpg, mp3, asf, ico, htm, hta, url, rm, com, vcf, ppt, rtf, chm, hlp и други.

Позиция	Минимални изисквания
REQ.25.	Решението трябва да предоставя „предварителен изглед“ на засечените съмнителни URL адреси, като трябва да може да предоставя на анализаторите screenshot-и от URL адресите.
REQ.26.	Решението трябва да може да извършва динамичен анализ за зловреден код, да може да се обновява и да може да му се предоставя нова информация за заплахи, дори в offline режим, без да има връзка с Интернет.
REQ.27.	Решението трябва да може да предоставя контекстуална информация към вдигнатите аларми, като например източник, степен на опасност, потенциални рискове, варианти за справяне с проблема и т.н., за засечените атаки от дадена рискова група.
REQ.28.	Решението трябва да разполага с голям набор от виртуални машини за sandbox анализ, с предварително инсталирани операционни системи и софтуер, бивайки Windows OS (включително 7, 10), Mac OSX и Linux Cent OS, с различни версии на Service Pack, 32 и 64 битови, за да може да извършва точен анализ на поведението на процесите според различните уязвимости на средите.
REQ.29.	Решението трябва да предоставя множество приложения с различни версии за тестове, разположени на виртуалните машини за анализ на зловредни файлове. Приложенията и версиите трябва да бъдат минимум следните: Microsoft Office 2003, 2007, 2010, 2013; Adobe Reader 7, 8, 9, 10, 11; Internet explorer 6, 7, 8, 9, 10, 11.
REQ.30.	Решението трябва да може да анализира един и същ файл на различни видове и версии на операционни системи и приложения, както и на различни версии на Internet Explorer, за да се открие потенциално зловредно поведение, използващо конкретни уязвимости.
REQ.31.	Решението трябва да може да алармира за зловредни процеси, които не са били засечени в първоначалните 24 часа, а на по-късен етап е установено, че са зловредни.
REQ.32.	След извършване на анализ, решението трябва да може да предоставя пълен отчет за него, който да съдържа минимално следната информация: • Тип на анализираните файлове; • Име на пробата; • Контролните суми на анализираните файлове (MD5, SHA1 / 256/512); • Класификация според това, към кое семейство се причислява засечения зловреден код; • Тип на използваната уязвимост за пробив; • URL адреси, които са използвани за атаката, както и предоставяне на информация за преглед на съдържанието на URL адресите чрез изображения (screenshots); • Данни за идентифициране на заразените системи (IP, MAC); • Графично изобразяване на поведението на анализирания зловреден код; • Извършени промени по операционните системи;

Позиция	Минимални изисквания
	• Извършени промени по инсталираните приложения на виртуалните машини за анализ; • Извършени промени по файловата система; • Извършени промени по регистрите на Windows операционните системи; • Качените DLL библиотеки; • Извиканите Windows API функции, в хронологичен ред; • Информация за създадените / модифицираните / спрените процеси; • Детайлно изобразяване на поведението на процесите на мрежово ниво в графичен формат (изпълнени мрежови свързвания и използваните транспортни мрежови протоколи, използвани портове, DNS заявки и отговори, http пакети); • Информация за IP адресите, с които е комуникирано;
REQ.33.	Решението трябва да може да съхранява данните от изпълнението на зловреден код и прилежащите артефакти, като например PCAP файл с данни от засечените заплахи, за да може информацията да се анализира допълнително и след извършения sandbox анализ.
REQ.34.	Решението трябва да може да се поставя в следните режими на работа: SPAN, TAP, inline или HW bypass.
REQ.35.	Решението трябва да позволява използването на YARA правила.
REQ.36.	Решението трябва да може да анализира мрежови трафик независимо от използваните VLAN и портове, без да изисква предварително задаване на параметри, включително да се поддържат протоколи Encapsulated remote SPAN, Virtual Extensible LAN и Internet Content Adaptation Protocol.
REQ.37.	Решението трябва да разполага с команден и с графичен интерфейс (достъпен през стандартен уеб-браузър) за централизирано управление, без да се изисква инсталиране на допълнителен софтуер.
REQ.38.	Решението трябва да поддържа ролево-базиран достъп до конзолата за управление. Да могат да се задават различни профили и права (администратор, оператор, одитор и т.н.), като да се задават кои отчети, аларми и информация могат да виждат в конзолата за управление.
REQ.39.	Решението трябва да може да анализира и засича атаки, които протичат на няколко нива и фази, а да не предоставя само sandbox технология за анализ на отделни файлове в изолация.
REQ.40.	Решението трябва да борави с различни версии на Microsoft Office във виртуалните машини за анализ, като да може да анализира Microsoft Office документи с вграден зловреден код или макроси за пароли, анализ на зловреден трафик от тях, както и да се засичат системни грешки, свързани с документите.
REQ.41.	Решението трябва да може да засича и класифицира следните категории атаки: • Ransomware криптиращи атаки; • Следи от meterpreter команди; • Кражба на файлове; • Инфектиране на файлове;

Позиция	Минимални изисквания
	• Опити за силово разбиване на пароли; • Изпълнение на команди; • Използване на уязвимости за пробив (exploit); • Атаки с цел разузнаване;
REQ.42.	Решението трябва да може да анализира причините за принудително спиране на дадено приложение.
REQ.43.	Решението трябва да може да получава информация за нови киберзаплахи от глобална система за информация на производителя.
REQ.44.	Решението трябва да може да получава системни обновления и обновления за виртуалниите машини за анализ, директно от уеб-базирания интерфейс за централизирано управление на решението.
REQ.45.	Решението трябва да предоставя информация за системните си показатели в графичния интерфейс за управление.
REQ.46.	Решението трябва да позволява използването на прокси сървър с оторизация за сваляне на обновления.
REQ.47.	Решението трябва да може с точност да идентифицира и обособи филтриран и блокиран мрежови трафик през уеб прокси.
REQ.48.	Решението трябва да позволява филтриране на мрежови трафик, да се определя, дали да се анализира или блокира трафикът, като се използват „бели списъци“. Трябва да може да се филтрира на базата на: Generic Routing Encapsulation, използвани портове за комуникация и филтриране на конкретни мрежи (по зададени IP адреси или подмрежи).
REQ.49.	Решението трябва да поддържа LDAP, TACACS + или RADIUS методи за вписване на потребителите.
REQ.50.	Решението трябва да може да използва XFF хедъри за идентифициране на коя машина генерира аларми, когато се намира зад прокси сървър.
REQ.51.	Решението не трябва да позволява мрежова комуникация от виртуалните машини за анализ към Интернет и от анализирания зловреден код към хакерски команден център или към URL адрес.
REQ.52.	По време на извършван анализ, ако зловредният код изпрати заявка за сваляне на допълнителни файлове (двоичен код), решението трябва да може да предостави на виртуалната машина заместващ доброкачествен файл, за да се продължи изпълнението и анализа.
REQ.53.	Решението трябва да може да предоставя следната информация: • Доклад с промените по системите; • Копие на зловредния двоичен код; • Мета данни от зловредния код; • Уловен мрежови трафик (PCAP файл) от виртуалните машини за анализ; • Пълно описание на достъпените URL адреси от зловредния код с идентифицирне на локациите им.
REQ.54.	Решението трябва да може да предоставя извличането на отчети и аларми в PDF формат.
REQ.55.	Решението трябва да може да определи степента на заплаха на даден инцидент от вдигнатите аларми за него.

Позиция	Минимални изисквания
REQ.56.	Решението трябва да може да вдига различни аларми за всяка фаза от жизнения цикъл на засечените атаки.
REQ.57.	Решението трябва да може да засича опити за използване на функциите за приспиване (sleep) на операционните системи от зловредния код и да може да забързва времето на виртуалните машини за анализ, за да принуди изпълнението на зловредния код.
REQ.58.	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.59.	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.60.	Решението трябва да може да изпраща известия за собственото си здраве и процеси, на базата на SMTP, до предварително зададени локации.
REQ.61.	Решението трябва да може да се интегрира (за обмен на информация) с другите решения на производителя.
REQ.62.	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.
Софтуерна поддръжка от производителя	
REQ.63.	Срок: **до 31.12.2030г.**
REQ.64.	Тип поддръжка: 24x7x365
REQ.65.	Възможност за обновление на софтуера в периода на поддръжката
REQ.66.	Възможност за обновления на информацията за заплахите от базата данни на производителя

Таблица № 32

Позиция	Изисквания за 2-та броя хардуерни устройства Trellix Web Security appliance (High-Availability) с вграден софтуер
REQ.67.	Производителност мрежова защита, мрежови трафик: минимално 6 Gbps
REQ.68.	Производителност на вградена IPS функционалност, мрежови трафик: минимално 6 Gbps
REQ.69.	Минимален брой поддържани едновременни сесии за IPS: 4M
REQ.70.	Минимален брой поддържани нови сесии в секунда за IPS: 80K/Sec
REQ.71.	Устройството да е с максимална големина 2RU
REQ.72.	Устройството да разполага с поне 10TB за съхранение на данни
REQ.73.	Устройството да поддържа следните режими на работа на портовете за наблюдение на мрежата: In-line Monitor, Fail-Open, Fail- Close (HW Bypass) или TAP/SPAN
REQ.74.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
Гаранция	

Позиция	Изисквания за 2-та броя хардуерни устройства Trellix Web Security appliance (High-Availability) с вграден софтуер
REQ.75.	Срок: **до 31.12.2030г.**
REQ.76.	Тип поддръжка: 24x7x365 (възможност за хардуерна подмяна при дефектирало устройство)
REQ.77.	Възможност за обновление на firmware-а на хардуерното устройство

1.4. Разширени функции за засичане на напреднали мрежови атаки, корелация на мрежови събития и вземане на ответни мерки

Таблица № 33

Позиция	Минимални изисквания
REQ.78.	Тип решение: **6 броя абонаментни лиценза до 31.12.2030г. Trellix Network Detection and Response (NDR) за разширени функции за динамичен анализ на зловреден код и защита от кибератаки на мрежово ниво за 6 Gbps мрежови трафик**, с включени **1 брой вирутално устройство за управление на NDR** и **1 брой виртуално устройство, служещо за мрежови сензор**, с вграден софтуер и поддръжка **до 31.12.2030г.**
REQ.79.	Решението трябва да предоставя разширени функции за засичане на напреднали мрежови атаки, корелация на мрежови събития и вземане на ответни мерки (NDR), с възможност за използване на различни видове сензори за събиране на мрежови данни: -виртуални устройства от същия производител с пълна функционалност -хардуерните устройства от решението за защита на мрежова среда от напреднали атаки от същия производител с пълна функционалност -интеграция с мрежови сензори от трети страни, за частично събиране на данни или обогатяване на аларми
REQ.80.	Решението трябва да може да събира метаданни от мрежовия трафик от едно и също устройство-сензор, както входящ за организацията (трафик север-юг), така и при движение настрани на мрежови процеси (трафик изток-запад) .
REQ.81.	Решението трябва да може автоматично да корелира цялата събрана информация, за да открива сложни мрежови атаки, протичащи на няколко фази.
REQ.82.	Решението трябва да може автоматично да предприема ответни мерки по предварително зададени логически схеми за автоматизация на мрежови устройства за киберсигурност и за защита на крайни точки при възникване на мрежова заплаха.
REQ.83.	Решението трябва периодично да получава информация за нови заплахи от прозиводителя като част от абонамента на решението.
REQ.84.	Решението трябва да може да агрегира множество индивидуални аларми като единна атака, ако са свързани, като трябва да може да поставя оценка на риска от всяка заплаха, със съответно оцветяване на събитията според степента им на риск, с възможност за детайлен

Позиция	Минимални изисквания
	преглед на всички събрани аларми от системите за мрежова киберсигурност, които са част от агрегираното събитие.
REQ.85.	Решението трябва да може да предоставя времедиаграми, където е приложимо, при засичане на заплахи, показващи коренния причинител и последвалите дъщерни процеси от дадената заплаха. Графичният интерфейс на решението трябва да позволява извеждане на повече детайли за всяка точка от времедиаграмата.
REQ.86.	Решението трябва да може да предоставя графики с мрежовите връзки между събитията, където е приложимо, за възникнали заплахи, показващи как мрежовите процеси са свързани и ясно обособено кои процеси са външни за организацията (трафик север-юг) и кои са свързани с движение настрани в организацията (трафик изток-запад).
REQ.87.	Решението трябва да може да изпраща извлечени елементи от мрежовия трафик за допълнителен sandbox анализ към лабораторията за ръчно или автоматизирано детайлно разследване на непознати, потенциално зловредни елементи и да може да предприема автоматични действия на базата на върнатия резултат от изследването.
REQ.88.	Решението трябва да може да анализира криптиран SSL трафик.
REQ.89.	Решението трябва да може да извършва пасивно откриване на всички мрежови активи на организацията.
REQ.90.	Решението трябва да може да извършва анализ и да открива пътя от започване на дадена атака (коренният причинител) до изпълнението на зловредната и фаза.
REQ.91.	Решението трябва да разполага с набор от автоматични действия по подразбиране (out-of-the-box), но да може да се създават и собствени процеси по автоматизация на отвени мерки при заплахи.
REQ.92.	Решението трябва да може да се интегрира с решението за детайлни анализи на мрежови потоци и мрежови пакети, за да може да улавя всички мрежови пакети, свързани с дадена заплаха и за да може да реконструира целите мрежови сесии за дадения период на възникване на дадената атака.
REQ.93.	Решението трябва да може да реконструира Netflow мрежови сесии.
REQ.94.	Решението трябва да разполага със собствен GenAI изкуствен интелект, специално създаден за работа с решението и с киберзаплахи, който да помага на администраторите, предоставяйки при поискване: -допълнителен контекст при възникнали аларми под формата на текстов отговор и метаданни -препоръки за подходящи ответни мерки при възникнал инцидент -извършване на автоматични ответни мерки при възникнал инцидент -създаване и предоставяне на специализирани графични отчети и диаграми за даден възникнал инцидент
REQ.95.	Решението трябва да включва използването на изкуствения интелект като част от абонамента на решението, без допълнителни такси, поне

Позиция	Минимални изисквания
	за определен брой (различен от нула) заявки на месец/година/за периода на ползване на решението, според лицензионния модел на производителя. Да има опция за закупуване на допълнителни заявки в бъдеще при необходимост.
Софтуерна поддръжка от производителя	
REQ.96.	Срок: **до 31.12.2030г.**
REQ.97.	Тип поддръжка: 24x7x365
REQ.98.	Възможност за обновление на софтуера в периода на поддръжката
REQ.99.	Възможност за обновления на информацията за заплахите от базата данни на производителя

Таблица № 34

Позиция	**Изисквания за 1 брой виртуално устройство за управление на NDR и 1 брой виртуално устройство, служещо за мрежови сензор**
REQ.100.	Виртуалните устройства да се предоставят в различни формати, минимално като OVA за поставяне под VMware ESXi (версии 6.5 или по-нови).
REQ.101.	**Гаранция**
REQ.102.	Срок: **до 31.12.2030г.**
REQ.103.	Тип поддръжка: 24x7x365
REQ.104.	Възможност за обновление на firmware-а на виртуалните устройства

1.5. Решение за детайлни анализи на мрежови потоци и мрежови пакети

Таблица № 35

Позиция	Минимални изисквания
REQ.105.	Тип решение: Подновяване и обновяване на **Trellix Network Forensics**, включващо: **1 брой хардуерно устройство за улавяне на мрежови пакети**, с вграден софтуер и включена поддръжка **до 31.12.2030г. 1 брой хардуерно устройство за допълнително дисково пространство за съхранение на мрежови пакети**, с вграден софтуер и включена поддръжка **до 31.12.2030г.; 1 брой абонамент за софтуерни лицензи и услуги към хардуерното устройство за допълнително дисково пространство за съхранение на мрежови пакети**, с включена поддръжка **до 31.12.2030г.;**; **1 брой хардуерно устройство за разследвания и централизиран анализ и визуализация,** с вграден софтуер и включена поддръжка **до 31.12.2030г.**;
REQ.106.	Решението трябва да има пълна видимост над мрежовия трафик, чрез високоскоростно улавяне на мрежови пакети и анализ на ниво gateway. Решението трябва да може да се поставя в TAP/SPAN режим на работа, като трябва да може да получава мрежовите данни след SSL декриптиране от настоящо решение за SSL декриптиране на организацията от трети производител (да има възможност за интеграция).

Позиция	Минимални изисквания
REQ.107.	Решението да има възможност за изключително бързо (в реално време) записване и индексиране на мрежови трафик.
REQ.108.	Решението трябва да може да улавя, търси и анализира информацията от мрежовите пакети и сесии.
REQ.109.	Решението трябва да може да чете и записва пакети в PCAP формат.
REQ.110.	Решението трябва да позволява извършването на филтрирани търсения, използвайки често срещани стойности за адрес, приложение, протокол, VLAN, MPLS, метаданни от мрежовата връзка.
REQ.111.	Решението трябва да поддържа интеграция с решението за защита на крайни потребители и сървъри, за да може да получава информация за вътрешно наблюдаваните IP адреси от крайните точки и за да може да извлича потребителските имена, асоциирани с дадено име на хост.
REQ.112.	Решението трябва да може да анализира мрежови сесии и да извлича файлове от тях.
REQ.113.	Решението трябва да позволява на анализаторите да търсят в мрежовия трафик ключови думи и регулярни изрази на ниво приложен слой.
REQ.114.	Решението трябва да поддържа сложни заявки, използващи булева логика.
REQ.115.	Решението трябва да може да се интегрира и изпраща извлечени файлове от мрежови сесии директно към подсистема (лаборатория) за динамичен анализ на зловреден код.
REQ.116.	Решението трябва да може да реконструира уеб-страници и email съобщения от уловения мрежови трафик. Също така трябва да може да реконструира POP3/IMAP/FTP/SMB.
REQ.117.	Решението трябва да може да извлича данни от много големи файлове с мрежови трафик, до 1 гигабайт.
REQ.118.	Решението трябва да може да кодира/декодира следните формати от данни: Base64, gzip, HEX, HEXDUMP, JSON, URL, XOR.
REQ.119.	Решението трябва да позволява определянето на собствени правила, на базата на които да се улавя и съхранява мрежовия трафик за по-нататъшен анализ.
REQ.120.	Решението трябва да може да анализира в детайли следните протоколи: DCE-RPC, IPv6, SMB, DHCP, IRC, SMB2, DNS, MODBUS, SMTP, ERSPAN, MPLS, SSL, FTP, MSN, SSH, GRE, POP3, TCP, HTTP, PPP, TEREDO, ICMPv4, RDP, TLS, ICMPv6, RTSP, UDP, IMAP, SCTP, VLAN, IPv4, SIP, IPFIX, NETFLOWv5, NETFLOWv9.
REQ.121.	Решението трябва да позволява търсене в индексираните метаданни на следните протоколи: HTTP, DNS, SMTP, POP3, IMAP, SSL, TLS, FTP, SSH и MODBUS.
REQ.122.	Решението трябва да може да разпознава минимално следните приложения: AFP, Aimini, Amazon, Apple, AppleiCloud, AppleiTunes,

Позиция	Минимални изисквания
	AppleJuice, Armagetron, AVI, Ayiya, BattleField, BGP, BitTorrent, CiscoSkinny, CiscoVPN, Citrix, Citrix_Online, CNN, Collectd, Corba, Crossfire, DCE_RPC, DHCP, DHCPV6, DirectConnect, Direct_Download_Link, DNS, Dofus, DropBox, eBay, eDonkey, EGP, EPP, Facebook, FacebookChat, FastTrack, Fiesta, Filetopia, Flash, Florensia, FTP, FTP_CONTROL, FTP_DATA, GMail, Gnutella, Google, GoogleMaps, GRE, GrooveShark, GTP, Guildwars, H323, HalfLife2, HTTP, HTTP_Application_ActiveSync, HTTP_APPLICATION_VEOHTV, HTTP_Connect, HTTP_Proxy, IAX, IceCast, ICMP, ICMPV6, IGMP, IMAP, IMAPS, iMESH, IPP, IPsec, IP_in_IP, IRC, Jabber, Kerberos, Kontiki, LastFM, LDAP, LLMNR, LotusNotes, MapleStory, MDNS, Meebo, Megaco, MGCP, MMS, Move, MPEG, MSN, MsSQL, MySQL, NetBIOS, NetFlix, NFS, NOE, NTP, OggVorbis, OpenFT, OpenVPN, Oracle, Oscar, OSPF, Pandora, Pando_Media_Booster, PcAnywhere, POP, POP3, POPS, PostgreSQL, PPLive, PPStream, PPTP, QQ, QQLive, Quake, QuickTime, Radius, RDP, RealMedia, Redis, RemoteScan, RSYNC, RTCP, RTMP, RTP, RTSP, SAP, SCTP, sFlow, ShoutCast, SIP, SkyFile_PostPaid, SkyFile_PrePaid, SkyFile_Rudics, Skype, SMB, SMTP, SMTPS, SNMP, SOCKS4, SOCKS5, Socrates, Sopcast, Soulseek, Spotify, SSDP, SSH, SSL, SSL_No_Cert, Stealthnet, Steam, STUN, Syslog, TDS, TeamSpeak, TeamViewer, Telegram, Telnet, TFTP, Thunder, TOR, TruPhone, Tuenti, Tvants, TVUplayer, Twitter, UbuntuONE, Unencryped_Jabber, Unknown, UPnP, Usenet, VEOHTV, VHUA, Viber, VMware, VNC, VRRP, Warcraft3, Webex, WebM, Whois-DAS, WhatsApp, Wikipedia, WindowsMedia, WindowsUpdate, WinMX, WorldOfKungFu,WorldOfWarcraft, Xbox, XDMCP, Yahoo, YouTube, Zattoo, ZeroMQ.
REQ.123.	Решението трябва да може да анализира следните видове мрежови трафик: използващ IPv4 протокол и използващ IPv6 протокол.
REQ.124.	Решението трябва да предоставя на администраторите разбираем и с възможност за модифициране интерфейс със списъци, графики и географски карти.
REQ.125.	Решението трябва да позволява на администраторите лесно и бързо да извършват „reverse DNS lookup“ и „whois“ проверки директно от уеб интерфейса.
REQ.126.	Решението трябва да позволява на анализаторите да преглеждат данните на ниво мрежова връзка, пакет и payload.
REQ.127.	Решението трябва да може да приема аларми от другите подсистеми за киберсигурност.
REQ.128.	Решението за улавяне на мрежови пакети трябва да използва „full disk encryption“ метод за криптиране на събраните данни и метаданни.
REQ.129.	Решението за улавяне на мрежови пакети трябва да може да се интегрира с SAS RAID или с HBA контролер, за да се гарантира непрекъснат процес на събирането на мрежови пакети.

Позиция	Минимални изисквания
REQ.130.	Решението трябва да разполага с IPMI интерфейс.
REQ.131.	Решението трябва да поддържа автентикация на потребителите с протоколи PAM/LDAP/RADIUS/TACACS+. Трябва да може да се поддържа ролево-базирано управление, потребителите да могат да имат различни роли (администратор, анализатор, т.н.)
REQ.132.	Решението трябва да може да засича извличане на данни извън организацията.
REQ.133.	Решението трябва да поддържа Suricata правила за дефиниции/алармиране.
REQ.134.	Решението трябва да позволява задаването на правила за филтриране на мрежовия трафик. Правилата са необходими за намаляване на обема анализиран трафик. Тези правила трябва да са наложени директно на хардуерните интерфейси за улавяне на трафика, преди да затормозят централния процесор на системата. Да може да се филтрира минимално на база следните параметри: src IP, src port, dst IP, dst port.
REQ.135.	Решението трябва да може да извлича метаданни от уловения мрежови трафик през HTTP.
REQ.136.	Решението трябва да може да индексира в реално време уловените мрежови пакети, използвайки маркери за време и атрибутите на мрежовите свързвания. Да могат да се извличат индекса на потока от данни и метаданните на мрежовата връзка в JSON формат.
REQ.137.	Решението трябва да предоставя информация за собствените си процеси и за складираните данни, за да може да се планира капацитета в бъдеще.
REQ.138.	Решението трябва да позволява да му се наблюдават параметрите по производителността чрез SNMP.
REQ.139.	Решението трябва да предоставя възможност за сигурно изтриване на данните от дисковото му пространство, чрез презаписване (overwrite) на данните множество пъти.
REQ.140.	Решението трябва да може да се интегрира с източници на информация за заплахи.
REQ.141.	Решението трябва да позволява добавянето на множество нови индикатори за компроментиране чрез формати STIX и OpenIOC.
REQ.142.	Решението трябва да позволява определяне на времеви интервал за автоматично търсене за индикатори за компроментиране в събраните метаданни и да може да вдига аларми за тях.
REQ.143.	Решението трябва да поддържа използването на reverse SSH и HTTPS тунели, за да може да се интегрира със системи от външна мрежа.
REQ.144.	Решението трябва да поддържа автентикация с използване на smart карти.
REQ.145.	Решението трябва да предоставя достъп за търсене в съхранените метаданни.

Позиция	Минимални изисквания
REQ.146.	Решението трябва да може да се интегрира и да приема метаданни на слой 7 от решението за защита на мрежова среда от напреднали атаки, както и да може да изисква уловени пакети по конкретно събитие, за което е вдигната аларма.
REQ.147.	Решението трябва да разполага с API интерфейс.
REQ.148.	Решението за улавяне на мрежови пакети трябва да е изградено с подсилена откъм сигурност, заключена операционна система.
REQ.149.	Решението да разполага с достатъчно дисково пространство за съхранение на събраната информация, с минуимум 500TB, така че да се постигне съхранение за период от минимално 14 дни назад на мрежовите данни.
Софтуерна поддръжка от производителя	
REQ.150.	Срок: **до 31.12.2030г.**
REQ.151.	Тип поддръжка: 24x7x365
REQ.152.	Възможност за обновление на софтуера в периода на поддръжката
REQ.153.	Възможност за обновления на информацията за заплахите от базата данни на производителя

Таблица № 36

Позиция	Изисквания към 1 бр. хардуерно устройство за улавяне на мрежови пакети
REQ.154.	Устройството да е с максимална големина 2U
REQ.155.	Устройството да разполага с поне 120TB за съхранение на данни, с възможност за разширяване на обема със скачено SAS дисково пространство
REQ.156.	Устройството да може да записва мрежови данни със скорост от 6Gbps
REQ.157.	**Гаранция**
REQ.158.	Срок: **до 31.12.2030г.**
REQ.159.	Тип поддръжка: 24x7x365 (възможност за хардуерна подмяна при дефектирало устройство)
REQ.160.	Възможност за обновление на firmware-а на хардуерното устройство

Таблица № 37

Позиция	Изисквания към 1 бр. хардуерно устройство за допълнително дисково пространство за съхранение на мрежови пакети
REQ.1.	Устройството да разполага с поне 450TB допълнително пространство за съхранение на данни
REQ.2.	**Гаранция**
REQ.3.	Срок: **до 31.12.2030г.**
REQ.4.	Тип поддръжка: 24x7x365 (възможност за хардуерна подмяна при дефектирало устройство)
REQ.5.	Възможност за обновление на firmware-а на хардуерното устройство

Таблица № 38

Позиция	Изисквания към 1 бр. хардуерно устройство за разследвания и централизиран анализ и визуализация
REQ.6.	Устройството да разполага с поне 80TB за съхранение на данни
REQ.7.	**Гаранция**
REQ.8.	Срок: **до 31.12.2030г.**
REQ.9.	Тип поддръжка: 24x7x365 (възможност за хардуерна подмяна при дефектирало устройство)
REQ.10.	Възможност за обновление на firmware-а на хардуерното устройство

1.6. Решение за засичане и защита от напреднали атаки във файлови хранилища

Таблица № 39

Позиция	Минимални изисквания
REQ.11.	Тип решение: Подновяване и обновяване на **Trellix File Security**, включващо: **1 брой хардуерно устройство с вграден софтуер** и включена поддръжка **до 31.12.2030г.**, **2 броя виртуални устройства с вграден софтуер** и включена поддръжка **до 31.12.2030г. ,** както и **1 брой абонамент с включена поддръжка до 31.12.2030г.**
REQ.12.	Решението трябва да може да анализира файлове, използвайки sandbox технология, която да може да засича непознат „zero-day" зловреден код, вграден във файловете.
REQ.13.	Решението трябва да може да получава автоматично данни за заплахи от засечени такива при други клиенти на производителя от цял свят.
REQ.14.	Решението трябва да може да извършва рекурсивни автоматични сканирания, сканирания по времеви график и сканирания по ръчна заявка от администратор, за всички достъпни мрежови файлови дялове, за да да може да идентифицира и сложи под карантина всички засечени вируси по съхранените файлове, без да има значително влияние върху производителността на системите.
REQ.15.	Решението да позволява задаването на различни настройки за всяко сканиране, като да могат да се задават различни файлови типове или конкретни файлове да могат да бъдат сложени в „бял списък", за да са изключени от сканирането.
REQ.16.	Решението трябва да позволява паузиране и продължаване на сканирания, които се извършват в даден момент (в реално време).
REQ.17.	Решението трябва да може да премества безопасните файлове в определени локации, а заразените файлове да може да премества в отделена карантина.
REQ.18.	Решението трябва да може да връща файлове в първоначалните им локации, след като са освободени от карантината.
REQ.19.	Решението трябва да може да издава пълни отчети за поведението на файловете – прилежащи процеси, достъп до файловете/записани файлове на дисковото пространство, промени в регистрите на операционната система.

Позиция	Минимални изисквания
REQ.20.	Решението трябва да може да споделя откритите от него индикатори за компроментиране с останалите подсистеми, за динамичен анализ на зловреден код и за разследвания за кибератаки, също така да може и да получава индикатори за компроментиране от тях.
REQ.21.	Решението трябва да предоставя настройки на филтри при сканирането на файлове, според типа на файловете, локацията им, последната дата на модифициране.
REQ.22.	Решението трябва да позволява използването на YARA правила, версия 3.4.
REQ.23.	Решението трябва да може да извършва освен динамичен анализ, така и статичен анализ. Администраторите трябва да могат да избират, дали да се извършва статичният анализ.
REQ.24.	Максималният размер на файловете, които ще се анализират, да може да бъде променян.
REQ.25.	Решението трябва да може да прави морфологичен разбор на .eml файлове.
REQ.26.	Решението трябва да може да извлича прикачени файлове от .eml файлове. Броят на прикачени файлове, които да се анализират, трябва да може да бъде променян.
REQ.27.	Решението трябва да може да създава локални дефиниции (signatures) на засечените зловредни файлове след динамичен анализ. Администраторите трябва да могат да конфигурират времето на изтичане на валидността на локалните дефиниции.
REQ.28.	Решението трябва да може да се интегрира по подразбиране с Microsoft Office 365 за обработка на файлове.
REQ.29.	Решението трябва да може да се интегрира по подразбиране с Microsoft OneDrive за обработка на файлове. Решението трябва да може да извършва динамичен анализ на файловете в облачното пространство на OneDrive.
REQ.30.	Решението трябва да може да се интегрира по подразбиране с Microsoft SharePoint Online, за защитено споделяне на файлове.
REQ.31.	Решението трябва да може да изпраща известия за събития по email, HTTP, Rsyslog, SNMP в XML, JSON или в текстов формат.
REQ.32.	Решението трябва да поддържа следните протоколи: CIFS, NFS, WebDAV, Secure WebDAV.
REQ.33.	Решението трябва да позволява избирането на кои файлови хранилища да се сканират директно от графичния интерфейс за управление.
REQ.34.	Решението трябва да може да извлича първоначална информация за споделените дискови пространства, като например брой и тип на файловете на тях, за да може по-лесно да се определят критериите за сканирането им от решението.
REQ.35.	Решението трябва да предоставя информация за резултатите след извършване на сканиране.

Позиция	Минимални изисквания
REQ.36.	Решението трябва да може да предоставя детайлни отчети във формати .xml, .json, .csf и текстов формат, както и обобщителни отчети в .pdf формат.
REQ.37.	Решението трябва да позволява определянето на времеви график за автоматично изготвяне и изпращане на отчети.
REQ.38.	Решението трябва да позволява лесно извличане на резултати от анализи в PDF формат.
REQ.39.	Решението трябва да поддържа ролево-базиран достъп до конзолата за управление.
REQ.40.	Решението трябва да може да се интегрира с решението за централизирано управление и да може да се конфигурира от нея. Трябва да могат да се получават системни обновления през решението за централизирано управление и да се обменят аларми и известия.
REQ.41.	Решението трябва да може да анализира файловете в локален sandbox, както и да може да изпраща файловете за анализ към външен sandbox, когато устройството е претоварено.
REQ.42.	Решението трябва да разполага с IPMI интерфейс.
REQ.43.	Решението трябва да поддържа AAA протокол за контрол на потребителския достъп.
REQ.44.	Решението трябва да разполага с вградени функции за филтриране на IP адреси, за да се защити интерфейсът за управление от нежелан достъп.
REQ.45.	Решението трябва да позволява определянето на използваните ресурси за sandbox анализ, за да се избегне претоварване на системата.
REQ.46.	Решението трябва да поддържа наблюдение на показатели чрез SNMP.
REQ.47.	Решението трябва да предоставя функции за защитено изтриване на съхранени данни.
REQ.48.	Решението трябва да може да извършва автоматичен анализ на поне 85000 потенциално зловредни обекта на ден.
REQ.49.	Решението трябва да може да докладва за опитите за мрежово свързване на анализираните обекти във виртуалните машини.
REQ.50.	Решението трябва да може да извършва следствен анализ на откритите зловредни файлове и да може да предоставя копие на бинарния им (двоичен) код, както и PCAP файл с опитите им за мрежови свързвания, заедно с всички посетени URL адреси.
REQ.51.	Решението трябва да може да извършва динамичен анализ за зловреден код, да може да се обновява и да може да му се предоставя нова информация за заплахи, дори в offline режим, без да има връзка с Интернет.
REQ.52.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението трябва да използва собствен, специално изграден хипервайзор.
REQ.53.	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques).

Позиция	Минимални изисквания
REQ.54.	Решението трябва да разполага с графичен интерфейс, където да се изобразяват пълните детайли от извършения анализ на зловреден код.
REQ.55.	Решението трябва да позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите трябва да могат да променят поне следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, използван Outlook акаунт, използвани език и часова зона.
REQ.56.	Решението трябва да може да тества и засича зловреден код в различни операционни системи на виртуалните машини за sandbox анализ, с различни версии на service pack, като да се поддържат както x64, така и x86 архитектури, под Windows и под Mac.
REQ.57.	Решението трябва да може да извършва детайлен анализ и да открива зловреден код в следните файлови формати (минимално): изпълними .exe файлове, JAVA, PDF, MS Office документи, често срещани мултимедийни файлови формати като JPEG, QuickTime, MP3, архиви тип ZIP/RAR/7ZIP/TNEF, 3gp, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm.
REQ.58.	Решението трябва да позволява на администраторите да посочат кои приложения във виртуалните машини за анализ да стартират кои файлови типове.
REQ.59.	Решението трябва да може да извършва цялостен анализ локално, без да е необходимо да излиза информация извън структурите на организацията.
REQ.60.	Решението трябва да поддържа LDAP или RADIUS методи за вписване на потребителите (минимално).
REQ.61.	Решението трябва да разполага с команден и с графичен интерфейс (достъпен през стандартен уеб-браузър) за централизирано управление.
REQ.62.	Решението трябва да може да работи в следните режими (за анализиране на файлове): · Сканиране по ръчни заявки (on-demand, с възможност и за анализ на отделни файлове) · Продължително сканиране на посочени файлови хранилища.
REQ.63.	Решението трябва да позволява избирането на различни локации за преместване на файлове след анализ според това, дали са със статус на „добър“, „неизвестен“ или „лош“.
Софтуерна поддръжка от производителя	
REQ.64.	Срок: **до 31.12.2030г.**
REQ.65.	Тип поддръжка: 24x7x365
REQ.66.	Възможност за обновление на софтуера в периода на поддръжката
REQ.67.	Възможност за обновления на информацията за заплахите от базата данни на производителя

Таблица № 40

Позиция	Изисквания към 1 брой хардуерно устройство с вграден софтуер
REQ.68.	Устройството да е с максимална големина 2RU
REQ.69.	Устройството да разполага с поне 4TB за съхранение на данни
REQ.70.	Устройството да може да анализира минимално 85000 файла на ден.
REQ.71.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
REQ.72.	**Гаранция**
REQ.73.	Срок: **до 31.12.2030г.**
REQ.74.	Тип поддръжка: 24x7x365 (възможност за хардуерна подмяна при дефектирало устройство)
REQ.75.	Възможност за обновление на firmware-а на хардуерното устройство

Таблица №41

Позиция	Изисквания към 2 броя виртуални устройства с вграден софтуер
REQ.76.	Устройствата да могат да анализират минимално 45000 файла на ден.
REQ.77.	**Гаранция**
REQ.78.	Срок: **до 31.12.2030г.**
REQ.79.	Тип поддръжка: 24x7x365
REQ.80.	Възможност за обновление на firmware-а на виртуалното устройство

1.7. Решение за централизирано анализиране в sandbox среда на данните от мрежовите сензори

Таблица № 42

Позиция	Минимални изисквания
REQ.81.	Тип решение: Подновяване и обновяване на **Trellix Forensics – Web**, включващо: **2 броя хардуерни устройства** с вграден софтуер и включена поддръжка **до 31.12.2030г.**
REQ.82.	Решението трябва да работи като sandbox engine, с възможност за получаване на заявки за анализ от други подсистеми за киберсигурност, както и директно, чрез API.
REQ.83.	Решението трябва да може да се интегрира с решението за централизирано управление, за да може да се споделя информация за засечените зловредни процеси с останалите подсистеми.
REQ.84.	Решението трябва да може да работи със специално написани (custom) YARA правила от версия 3.4.
REQ.85.	Решението трябва да разполага с различни методи за статичен анализ, като администраторите да могат да избират кои от тях да се използват.
REQ.86.	Решението трябва да може да алармира за зловредни процеси, които не са били засечени в първоначалните 24 часа, а на по-късен етап е установено, че са зловредни.
REQ.87.	Решението трябва да поддържа AAA протокол за контрол на потребителския достъп.
REQ.88.	Решението трябва да разполага с IPMI интерфейс.

Позиция	Минимални изисквания
REQ.89.	Решението трябва да предоставя вградена възможност за защита на интерфейса за управление чрез firewall правила за ограничаване на мрежовия трафик от неоторизирани източници.
REQ.90.	Администраторите трябва да могат да обновяват решението без връзка с Интернет – в изолирана мрежа.
REQ.91.	Решението трябва да поддържа наблюдение чрез SNMP v3.
REQ.92.	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н., решението трябва да използва собствен, специално изграден хипервайзор.
REQ.93.	Решението трябва да може да получава автоматично данни за заплахи от засечени такива при други клиенти на производителя от цял свят.
REQ.94.	Решението трябва да може да създава локални дефиниции (signatures) на засечените зловредни файлове. Администраторите трябва да могат да конфигурират времето на изтичане на валидността на локалните дефиниции.
REQ.95.	Решението трябва да позволява модифициране на параметрите на Outlook акаунта, използван в sandbox средата.
REQ.96.	Решението трябва да може да засича webshell скриптове.
REQ.97.	Решението трябва да може да изпълнява файлове, създадени от MS Office документи в startup директорията на операционната система по време на sandbox анализа.
REQ.98.	Решението трябва да може да изпълнява планираните (scheduled) задачи от зловредния код в sandbox средата.
REQ.99.	Решението трябва да позволява на администраторите да конфигурират датата и часа (времевата зона) и използвания език в sandbox средата.
REQ.100.	Решението трябва да може да извлича URL адреси от паметта по време на sandbox анализа.
REQ.101.	Решението трябва да може да извлича URL адреси от Microsoft Office файлове и от XPS файлове.
REQ.102.	Решението трябва да може да извлича и анализира свързани Relationship URL адреси.
REQ.103.	Решението трябва да може да засича зловредни Microsoft Office файлове с вградено видео в тях.
REQ.104.	Решението трябва да може да извършва анализ на следните специални файлови типове: REG, Microsoft Access, One Note, HTA и Scriptlet.
REQ.105.	Решението трябва да може да анализира Microsoft Office файлове, които са защитени с парола.
REQ.106.	Решението трябва да може да засича инжектиране на код.
REQ.107.	Решението трябва да може да извършва анализ на файлове, използвайки различни версии на Microsoft Office на виртуалните машини за sandbox анализ.
REQ.108.	Решението трябва да може да извлича и анализира вградени файлове в Microsoft Office файлове.

Позиция	Минимални изисквания
REQ.109.	Решението трябва да може да наблюдава PowerShell дейностите в sandbox средата и да може да докладва за тях.
REQ.110.	Решението трябва да може да извлича файлове, създадени от PowerShell процеси.
REQ.111.	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques) от зловредните процеси, като например PING проверки, проверки за време и техники с диалогови прозорци.
REQ.112.	Решението трябва да може да засича нови криптовируси (ransomware) в sandbox средата – без да има дефиниции (signatures) за тях.
REQ.113.	Решението трябва да поддържа Microsoft Windows 10 за засичане на drive-by атаки.
REQ.114.	Решението трябва да може да засича Point of Sale зловредни процеси.
REQ.115.	Решението трябва да може да засича зловредни процеси, използващи kernel уязвимости.
REQ.116.	Решението трябва да може да засича DDE атаки.
Софтуерна поддръжка от производителя	
REQ.117.	Срок: **до 31.12.2030г.**
REQ.118.	Тип поддръжка: 24x7x365
REQ.119.	Възможност за обновление на софтуера в периода на поддръжката
REQ.120.	Възможност за обновления на информацията за заплахите от базата данни на производителя

Таблица № 43

Позиция	Изисквания към 2-та броя хардуерни устройства с вграден софтуер за централизирано анализиране в sandbox среда на данните от мрежовите сензори
REQ.121.	Необходими са **2 броя хардуерни устройства**, които да могат да поемат процесите по анализиране на зловреден код.
REQ.122.	Устройството да е с максимална големина 2RU
REQ.123.	Устройството да разполага с поне 4TB за съхранение на данни
REQ.124.	Устройството да може да извършва минимално 85 анализа в минута.
REQ.125.	Устройството да работи в изолиран режим, без Интернет свързаност. Устройството да не изпраща данни към производителя за засечените заплахи в организацията.
REQ.126.	**Гаранция**
REQ.127.	Срок: **до 31.12.2030г.**
REQ.128.	Тип поддръжка: 24x7x365 (възможност за хардуерна подмяна при дефектирало устройство)
REQ.129.	Възможност за обновление на firmware-а на хардуерното устройство

1.8. Решение за централизирано управление на всички компоненти от системата

Таблица № 44

Позиция	Минимални изисквания
REQ.1.	Тип решение: Подновяване и обновяване на **Trellix Central Management**, включващо: **1 брой хардуерно устройство**, **1 брой постоянен лиценз за софтуера с 1 брой поддръжка към хардуерното устройство** и **1 брой абонамент с включена поддръжка до 31.12.2030г. за цялото решение.**
REQ.2.	Решението трябва да може да извършва корелация на аларми между другите решения на производителя, за да се предостави защита от атаки, които се изпълняват на няколко нива и през няколко вектора. Например: атака чрез зловреден URL адрес, предоставен чрез съдържанието на електронно email съобщение, с прилежащ свален през уеб трафик зловреден файл, който е изпълнен на крайна точка, довело до нейното заразяване.
REQ.3.	Решението трябва да може да предоставя и изпълнява обновления на системния софтуер на управляваните от него подсистеми, да може предоставя на подсистемите обновления на информацията за нови заплахи и нови индикатори за компроментиране от глобалната система за информация на производителя или от трети източници.
REQ.4.	Решението трябва да поддържа интеграция с лабораторията за ръчно или автоматизирано детайлно разследване на непознати, потенциално зловредни елементи, за обмен на информация.
REQ.5.	Решението трябва да може да предоставя детайлни отчети, включително и обединена информация от управляваните подсистеми от решението.
REQ.6.	Решението трябва да може да управлява генерираните аларми от управляваните подсистеми и да може да изпраща известия, таблици и графики с данните от тях.
REQ.7.	Решението трябва да предоставя единна конзола, от която да може да се извършва централизирано конфигуриране на управляваните подсистеми, задаване на политики за сигурност, обновяване на информацията за заплахите / индикаторите за компроментиране, обновяване на системния софтуер на подсистемите.
REQ.8.	Решението трябва да позволява обновяване на управляваните подсистеми и информацията за нови заплахи дори в offline режим, без да е необходима свързаност с Интернет.
REQ.9.	Решението трябва да предоставя интегрирана централизирана администрация, в реално време, използвайки графичен интерфейс, който да предоставя следните функции: • Преглед и филтриране на събития, свързани със сигурността; • Идентифициране на заразени устройства; • Централизиране на всички известия и аларми от управляваните подсистеми; • Персонализиране на графичното изобразяване на информацията (персонализиране на dashboards); • Създаване и извличане на отчети в PDF и HTML формати.
REQ.10.	Решението трябва да позволява използването и дистрибутирането на индикатори за компроментиране от трети източници (индикатори, които

Позиция	Минимални изисквания
	могат да бъдат URL адреси, IP адреси, домейни и хеш суми на зловредни файлове) към управляваните подсистеми. Индикаторите за компроментиране трябва да могат да се управляват или чрез използването на списъци за всяка категория или чрез използването на STIX (Structured Threat Information Expression) формат.
REQ.11.	Решението трябва да поддържа LDAP, TACACS + или RADIUS методи за вписване на потребителите, както и чрез Активна Директория или решения за двуфакторна автентикация.
REQ.12.	Решението трябва да може да създава, съхранява и предоставя log файлове към трети решения, използвайки Syslog протокол, например за предоставяне на информация на решения от тип SIEM.
Софтуерна поддръжка от производителя	
REQ.13.	Срок: **до 31.12.2030г.**
REQ.14.	Тип поддръжка: 24x7x365
REQ.15.	Възможност за обновление на софтуера в периода на поддръжката
REQ.16.	Възможност за обновления на информацията за заплахите от базата данни на производителя

Таблица № 45

Позиция	Изисквания към 1 брой хардуерно устройство с вграден софтуер за централизирано управление на другите решения за защита
REQ.17.	Устройството да е с максимална големина 2RU
REQ.18.	Устройството да разполага с поне 4TB за съхранение на данни
REQ.19.	Устройството да може да управлява другите устройства за защита на крайни точки, за мрежова защита и за email защита, като всички те трябва да бъдат от един производител
REQ.20.	**Гаранция**
REQ.21.	Срок: **до 31.12.2030г.**
REQ.22.	Тип поддръжка: 24x7x365 (възможност за хардуерна подмяна при дефектирало устройство)
REQ.23.	Възможност за обновление на firmware-а на хардуерното устройство

1.9. *Изисквания към изпълнението*

Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или официален негов представител за право на разпространение на предлаганите продукти и услуги на територията на Република България.

VI. Други изисквания към проекта

1. Навсякъде в Техническите параметри – Приложение № 1, където се съдържа посочване на конкретен модел, източник, процес, търговска марка, патент, тип, произход, стандарт или производство да се чете и разбира „или ЕКВИВАЛЕНТ“.

2. Всички доставени софтуерни продукти по настоящия проект следва бъдат издадени на името на НАП.

3. Оборудването трябва да съответства или да надвишава в техническо отношение посочените минимални изисквания в настоящите Технически параметри – Приложение № 1.

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

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

6. Хардуерът следва да бъде доставен в пълно работно състояние, в оригиналната опаковка на производителя с ненарушена цялост, окомплектован с всички необходими интерфейсни и захранващи кабели, където се изискват, както и с необходимата техническа документация (на електронен носител или чрез линкове, от които може да бъде свалена).