Друштво за програмирање и консалтинг
СИГМОИД ГРОУП ДООЕЛ
бр. 0307-18-2025
09.10.2025 год.
СКОПЈЕ

Република Северна Македонија
Министерство за финансии

Архивски број: 03-11184/1
Датум:

08-10-2025

ДОГОВОР
за јавна набавка на стоки – софтвер за заштита на крајни корисници / сервер-next generation

Склучен помеѓу:

1.МИНИСТЕРСТВО ЗА ФИНАНСИИ, со седиште на ул.„Даме Груев“, бр.12 - Скопје, претставувано од м-р Гордана Димитриеска - Кочоска, министер за финансии, во натамошниот текст: договорен орган и

2.Друштво за програмирање и консалтинг СИГМОИД ГРОУП ДООЕЛ Скопје, со седиште на ул.„Перо Наков“ бр.122А/1-1-Каро Бизн Скопје, претставувано од Јован Јанкуловски, управител, во натамошниот текст: носител на набавката.

I. ПРЕДМЕТ НА ДОГОВОРОТ

Член 1

Предмет на овој договор е набавка на стоки – софтвер за заштита на крајни корисници / сервер - next generation, по спроведената поедноставена отворена постапка за набавка по оглас бр.13849/2025.

Предметот на договорот опфаќа и инсталација на антивирусен софтвер со вклучени лиценци за период од 1 (една) година, ремоте обука за користење на системот на вработените во договорниот орган, како и минимум 1 (еден) ден ремоте во месецот за консултации во времетраење на претплатата, во согласност со Техничките спецификации (Прилог 1 кон Договор) и Техничката понуда на носителот на набавката (Прилог 2 кон Договор).

Комерцијалното име на софтверот за заштита на крајните корисници е Check Point Harmony Endpoint Advanced.

II. ВРЕДНОСТ НА ДОГОВОРОТ

Член 2

Вкупната вредност на договорот без пресметан данок на додадена вредност изнесува 3.198.000,00 денари.

Вкупниот износ на данокот на додадена вредност изнесува 159.900,00 денари.

Вкупната вредност на договорот со пресметан данок на додадена вредност изнесува 3.357.900,00 денари.

III. ВАЖНОСТ НА ДОГОВОРОТ

Член 3

Договорот важи од денот на потпишување од двете договорни страни па се до истекот на лиценците за софтверот за заштита на крајни корисници чие времетраење е 1 (една) година сметано од денот на активирањето.

IV. РАЗЛИКА ВО ЦЕНА (КОРЕКЦИЈА НА ЦЕНИ)

Член 4

При реализација на договорот за јавна набавка не се предвидува корекција на цените, односно цените искажани во понудата на носителот на набавката ќе бидат фиксни за целото времетраење на договорот.

Во понудените цени се опфатени сите трошоци и тоа патните, дневните или евентуално други трошоци на носителот на набавката.

V. НАЧИН И РОК НА ИСПОРАКА

Член 5

Носителот на набавката е должен софтверот да го испорача, инсталира и конфигурира во период од 15 (петнаесет) работни денови по добивање на писмената порачка од страна на договорниот орган.

За извршената испорака, инсталација и конфигурација договорните страни потпишуваат документ - Работен налог/Записник, кој мора да ги содржи податоците за испорака, инсталација и конфигурација на софтверот.

Работниот налог/Записник за извршената испорака со полно име и презиме ги потпишуваат определените лица од двете договорни страни, при што по еден примерок се предава на задолженото лице за реализација кај договорниот орган,

еден примерок задржува носителот на набавката за сопствени потреби и еден примерок заедно со фактурата се доставува до договорниот орган.

VI. ГАРАНЦИЈА ЗА НАВРЕМЕНО И КВАЛИТЕТНО ИЗВРШУВАЊЕ НА ДОГОВОРОТ

Член 6

Носителот на набавката е должен заедно со потпишаниот договор да достави банкарска гаранција за квалитетно и навремено извршување на договорот.

Банкарската гаранција за квалитетно и навремено извршување на договорот треба да биде во висина од 5% од вкупната вредност на договорот со пресметан данок на додадена вредност и да е со важност до целосно реализирање на договорот.

Гаранцијата се доставува во вид на банкарска гаранција во писмена форма или во електронска форма доколку е издадена како таква од банката во изворно оригинална форма. Гаранцијата треба да биде поднесена во оригинална форма. Копии не се прифаќаат.

Гаранцијата за квалитетно и навремено извршување на договорот треба да биде со важност до целосното реализирање на договорот.

Банкарската гаранција за квалитетно и навремено извршување на договорот ќе биде во валутата на која гласи договорот.

Гаранцијата за квалитетно и навремено извршување на договорот треба да биде издадена од банка.

Гаранцијата за квалитетно и навремено извршување на договорот носителот на набавката ја доставува заедно со потпишаниот договор во рок од 5 работни дена од денот на добивање на договорот од страна на договорниот орган.

Гаранцијата за квалитетно и навремено извршување на договорот се доставува во определениот рок, и тоа: по пошта или лично на лицето за контакт определено од страна на договорниот орган.

Со оваа гаранција носителот на набавката гарантира дека предметот на договорот ќе го испорачува на начинот и според динамиката предвидени во тендерската документација, односно техничката спецификација, доставената понуда и склучениот договор со договорниот орган.

Гаранцијата за квалитетно и навремено извршување на договорот ќе биде наплатена доколку носителот на набавката не исполни некоја од обврските од договорот за јавна набавка во рокот на стасаноста, за што писмено ќе го извести носителот на набавката.

Министерство за финансии
Република Северна Македонија
Ул. „Даме Груев“ бр.12, Скопје
+389 2 3255 633
www.finance.gov.mk

Доколку договорот за јавна набавка е целосно реализиран согласно договореното, банкарската гаранција за квалитетно и навремено извршување на договорот договорниот орган му ја враќа на носителот на набавката во рок од 14 дена од целосното реализирање на договорот.

Гаранцијата за квалитетно и навремено извршување на договорот договорниот орган му ја враќа на носителот на набавката по пошта, лично во седиштето на носителот на набавката или лично во седиштето на договорниот орган.

Договорниот орган ќе ја наплати гаранцијата за квалитетно и навремено извршување на договорот и доколку дојде до негово едностранo раскинување поради неизвршување на обврските од договорот од страна на носителот на набавката.

Договорниот орган нема да бара активирање на банкарската гаранција за квалитетно и навремено извршување на договорот од банката која ја има издадено доколку носителот на набавката поради непредвидени околности (виша сила или други оправдани причини) не можел да ја изврши набавката што е предмет на овој договор, во кој случај носителот на набавката треба да достави писмено образложение до договорниот орган во кое ќе ги наведе причините за неизвршување или ненавремено извршување на набавката, а кое треба да биде писмено прифатено од договорниот орган.

VII. НАЧИН И РОК НА ПЛАЌАЊЕ

Член 7

Договорниот орган плаќањето ќе го изврши во рок до 30 (триесет) дена од денот на доставувањето на фактурата за извршената набавка, во писарницата на Министерството за финансии на ул. „Даме Груев" бр.12 во Скопје.

Кон фактурата носителот на набавката задолжително доставува Работен налог/Записник кој мора да содржи податоци за извршувањето на предметот на договорот, во спротивно фактурата нема да биде платена и ќе биде вратена на докомплетирање кај носителот на набавката.

Работниот налог/Записникот треба да биде потпишан со полно име и презиме од определените лица од двете договорни страни.

Фактурата се доставува по пошта или лично во писарницата на Министерството за финансии, на ул. Даме Груев бр.12 во Скопје.

VIII. ПРАВА И ОБВРСКИ НА НОСИТЕЛОТ НА НАБАВКАТА

Член 8

Носителот на набавката е должен своите обврски да ги извршува стручно, навремено и квалитетно, врз основа на барањата на договорниот орган дефинирани во техничките спецификации кои се составен дел од овој договор и техничката понуда прифатена од договорниот орган.

Носителот на набавката е должен да се придржува кон рокот за испорака и инсталација на софтверот, кој е дефиниран во член 5, став 1 од овој договор.

Носителот на набавката се обврзува предметот на договорот да го извршува со разумно знаење и внимание во согласност со професионалните стандарди и тековната легислатива која влијае на друштвата за компјутерски инжинеринг и трговија.

Носителот на набавката е должен веднаш по потпишување на договорот да му достави на договорниот орган податоци (име и презиме, матичен број и број на лична карта) за лицата кои ќе бидат определени за реализација на договорот.

IX. ПРАВА И ОБВРСКИ НА ДОГОВОРНИОТ ОРГАН

Член 9

Договорниот орган е должен да определи лица задолжени за реализација на договорот и за истото да го извести носителот на набавката.

Договорниот орган се обврзува дека плаќањето на носителот на набавката ќе го врши во согласност со членот 7 на овој договор.

Договорниот орган се обврзува да му ги даде на располагање на носителот на набавката потребните податоци за непречено извршување на договорот, како и друга документација со која располага вклучувајќи ја комуникацијата и сите други информации и објаснувања кои се потребни на носителот на набавката.

X. ДОВЕРЛИВОСТ НА ИНФОРМАЦИИ И ПОДАТОЦИ

Член 10

Определените лица од носителот на набавката за реализација на договорот, задолжително потпишуваат Изјава за доверливост на информации и податоци непосредно пред испораката на стоката - предмет на договорот.

Под поимот информации и податоци се подразбираат сите внатрешни и надворешни документи, спецификации, лични податоци, истражувања на пазарот или податоци за него, финансиски или маркетиншки информации, други податоци или бизнис, оперативни или технички информации, како и сите

останати податоци и информации и независно дали се дадени во писмена, вербална или електронска форма и се во сопственост на договорниот орган.

Исто така, поимот информации и податоци, ги опфаќа и сите други податоци кои не се сопственост на договорниот орган, а се користат за одредени цели во работните задачи и обврски. Тука спаѓаат податоци на сите партнери, клиенти, добавувачи или било кое правно или физичко лице кое со договорниот орган има засновано деловен или било каков друг однос. Договорниот орган ги става податоците на располагање на носителот на набавката во врска со погоре наведената цел, а за непречено одвивање на работните задачи и обврски.

Член 11

Не се предмет на овој договор информации кои биле или станале јавно достапни, но не како резултат на откривање од страна на носителот на набавката и на договорниот орган и без да бидат прекршени одредбите на овој договор од страна на носителот на набавката што може да се докаже со писмена документација или за кои договорниот орган писмено потврдил дека се ослободени од обврска за неоткривање.

Член 12

Носителот на набавката под целосна морална, материјална и кривична одговорност, се обврзува за време на важноста на договорот и во период од (5) пет години од датумот на неговото истекување или раскинување да ги чува во тајност сите информации и податоци од било која област на договорниот орган, кои ќе му бидат дадени во процесот на соработката и притоа нема да ги искористи истите за лични цели, во име на друго лице, ниту ќе ги даде на увид на трета страна.

Носителот на набавката се обврзува да ги чува во тајност сите документи и податоци кои содржат информации за договорниот орган или неговите активности, како и неговите односи со клиенти или трети лица, а кои биле подготвени или изнесени во врска со работата за која носителот на набавката е ангажиран од страна на договорниот орган.

Член 13

Носителот на набавката може да ги открие кои било од информациите и податоците наведени во членот 10 став 2 и 3 заради постапување по писмено барање од страна на надлежен орган, со легитимна наредба врз основа на закон.

Носителот на набавката, пред да ги даде бараните податоци ќе се увери дека барањето е валидно и е во согласност со важечки закон и ќе ги открие ваквите податоци само до степен до кој тоа е барано од надлежниот орган кој има овластување да бара такво соопштување.

Член 14

За секој настан или сомневање во однос на закана за нарушување на доверливоста, интегритетот и расположливоста на податоците и информациите, носителот на набавката се обврзува веднаш писмено да го извести определеното лице кај договорниот орган.

Член 15

Носителот на набавката по писмено барање на договорниот орган веднаш ќе ги врати или уништи сите документи кои содржат податоци и информации за договорниот орган, а кои се добиени во врска со работата за која носителот на набавката е ангажиран од страна на договорниот орган, без задржување на било какви фотокопии, изводи или друг вид на копии од нив или дел од нив. И покрај уништувањето на било кој податок и материјали носителот на набавката ќе продолжи да се придржува кон неговата обврска од овој договор и други обврски кои произлегуваат од него, за чување во тајност на сите податоци и информации кои ги сознал на било кој начин, при исполнување на неговите обврски кои произлегуваат од овој договор.

Член 16

Објавувањето податоци, рекламирањето или публицитетот, како и прес конференциите направени од страна на носителот на набавката во однос на овој договор или вршење на заеднички деловни активности на договорните страни треба да бидат претходно одобрени од договорниот орган пред нивното спроведување.

Член 17

Одредбите од глава X од овој договор се правно валидни и обврзувачки и кај сите вработени кај Носителот на набавката кои имаат добиено овластување за користење на информациите и податоците кои се уредени со овој договор.

XI. УСЛОВИ ЗА РАСКИНУВАЊЕ НА ДОГОВОРОТ

Член 18

Овој договор може да се раскине спогодбено, во согласност со договорните страни.

Министерство за финансии
Република Северна Македонија
Ул. „Даме Груев“ бр.12, Скопје
+389 2 3255 633
www.finance.gov.mk

Член 19

Овој договор може да се раскине и едностранo поради непридржување или неисполнување на договорните обврски утврдени со овој договор.

Договорната страна која поради непридржување или неисполнување на договорните обврски го раскинува договорот, должна е тоа да и го соопшти на другата договорна страна без одлагање во писмена форма.

Договорот се смета за раскинат со денот на приемот на известувањето за раскинување на договорот.

Доколку дојде до раскинување на договорот поради неисполнување или ненавремено исполнување на обврските на договорот од страна на носителот на набавката, покрај наплатата на гаранцијата за квалитетно и навремено извршување на договорот, носителот на набавката ќе биде одговорен за евентуалната штета што би ја предизвикал на договорниот орган како директна или индиректна последица на неговото работење.

Член 20

Кога една од договорните страни нема да ја исполни својата обврска, другата договорна страна може да бара исполнување на обврската од другата договорна страна или да го раскине договорот, а во секој случај има право на надомест на штетата.

Член 21

Кога договорната страна нема да ја исполни својата обврска во определениот рок, другата договорна страна може да и остави примерен дополнителен рок за исполнување на обврската.

Рокот од став 1 на овој член може да биде продолжен само по писмено барање на носителот на набавката и писмена согласност на договорниот орган.

Ако договорната страна која не ја исполнила својата обврска во определениот рок, не ја исполни обврската ни во дополнителниот рок, другата договорна страна може да го раскине договорот.

XII. ВИША СИЛА

Член 22

Ниту една од договорните страни нема да биде одговорна за неисполнување на обврските од овој договор до кое би дошло заради виша сила.

Под виша сила се подразбираат настани или околности на кои договорните страни не можат да влијаат и се надвор од нивната контрола, а го попречуваат нормалното извршување на договорот (елементарни непогоди, воени дејства, граѓански немири, штрајкови и сл.).

Вишата сила не вклучува настан што е предизвикан од небрежност или намерна активност што би предизвикала застој во извршувањето на обврските од договорот.

Ако една од договорните страни е спречена да ги исполнува своите обврски заради виша сила, должна е веднаш писмено да ја извести другата страна, со наведување на причините за вишата сила и по можност обезбедување на соодветен доказ.

За времетраењето на вишата сила сите права и обврски од овој договор мируваат.

Договорните страни се обврзуваат на ист начин да ја известат договорната страна за повторното воспоставување на нормални услови за извршување на договорот, односно за престанокот на дејството на вишата сила.

По отстранувањето на вишата сила договорот продолжува да се реализира.

XIII. ЗАВРШНИ ОДРЕДБИ

Член 23

Изменувања и дополнувања на договорот можат да се вршат со заедничка согласност на договорните страни по писмен пат.

Договорната страна која бара измена и/или дополнување на договорот е должна своето барање до другата страна да го достави во писмена форма.

Договорот може да се изменува и дополнува со анекс на договорот потпишан од двете договорни страни во согласност со Законот за јавните набавки.

Член 24

Ниту една договорна страна нема право своите обврски да ги пренесе на третата страна, без заемна писмена согласност.

Член 25

За сé што не е предвидено со овој договор, се применуваат одредбите од Законот за облигационите односи, Законот за јавните набавки и од другите позитивни прописи во Република Северна Македонија.

Член 26

Во случај на спор, договорните страни се согласни спорот да го решат спогодбено, а доколку во тоа не успеат, согласни се спорот да го решава предметно надлежниот суд во Скопје.

Член 27

При секоја обработка на личните податоци во текот на реализацијата на овој договор, соодветно ќе се применуваат одредбите од Законот за заштита на личните податоци.

Член 28

Овој договор е составен во 4 (четири) еднообразни примероци од кои 2 (два) примероци за договорниот орган и 2 (два) за носителот на набавката.

ДОГОВОРЕН ОРГАН:	НОСИТЕЛ НА НАБАВКАТА:
РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА МИНИСТЕРСТВО ЗА ФИНАНСИИ СКОПЈЕ	Друштво за програмирање и консалтинг СИГМОИД ГРОУП ДООЕЛ СКОПЈЕ
Министер за финансии	Управител
м-р Гордана Димитриеска – Кочоска	Јован Јанкуловски

Изработил: Панче Чоневски
Контролирал: Рената Николоска
Даниела Јанкова
Проверил: м-р Маја Стаменковска Угриновска
Михајло Михајловски
Проверил: Андреј Ангеловски
Владимир Стојанов
Ирена Петковски
Согласен: д-р Андриана Матлиоска

ПРИЛОГ 1

Технички спецификации

ТЕХНИЧКИ СПЕЦИФИКАЦИИ

Предмет на Договорот е набавка и инсталација на антивирусен софтвер со вклучени лиценци за период од 1 (една) година за:

- 650 работни станици (Windows 7, 8, 10 и Mac OC);

- 75 сервери (Windows Server 2008, 2012, 2016, Windows Server 2019 Data Center or Standard).

На 4 од серверите ќе биде поставен Microsoft Exchange Server, па антивирус софтверот и лиценците мора да бидат компатибилни со тие сервери на кој ќе биде поставен Microsoft Exchange Serverot и треба да ја нуди потребната заштита.

Техничка спецификација	
Контрола на пристап	
Огнен ѕид	Огнен ѕид за контрола на мрежниот сообраќај до и од крајните уреди, врз база на IP адреси домени, порти и и протоколи.
Контрола на апликации	Контрола на мрежен пристап за одредени апликации. Правилата за контрола на апликации овозможуваат дозволување, блокирање или терминирање на апликации и процеси.
Усогласеност на крајниот уред	Проверка дали уредот е во согласност со безбедносните правила на организацијата. Администраторот може да постави рестриктивни политики за неусогласените уреди.
VPN за оддалечен пристап	VPN за оддалечен пристап којшто им овозможува на корисниците кои што работат од далечина безбедносен пристап и користење на апликации што се наоѓаат во корпоративниот податочен центар. Целиот сообраќај што корисниците го примаат и праќаат треба да биде шифриран. Оваа функционалност треба да биде компатибилна со безбедносниот уред што го користи Договорниот орган.
Заштита од закани	

Заштита од ransomware	Постојано следење за специфично однесување на ransomware и идентификација на неодобрено шифрирање на датотеки без користење на дефиниции. Сите елементи на ransomware нападот се идентификувани преку форензичка анализа и се ставени во карантин - Враќање на податоци - шифрираните датотеки автоматски се враќаат од претходни snapshots - Intel TDT - имплементирана заштита на ниво на процесор со користење на Intel Threat Defense Technology.
Anti-Malware	Заштита од сите видови на злонамерни програми, од црви и тројанци до adware и keystroke loggers.
Anti-Bot	Детекција и превенција на закани од ботови.
Anti-Exploit	Заштита од напади базирани на ранливости во легитимни апликации и исклучување на злоупотребениот процес при детекција на истото
Behavioral Guard	Адатаптивна детекција и блокирање на мутации на злонамерни програми врз основа на нивното однесување во реално време
Заштита на влезно/излезните портови на крајниот уред	Контрола за поврзување на периферни уреди (тастатура, монитор, bluetooth, печатачи, Smart Card, мрежни адаптери, глувчиња итн.
Заштита на на Интернет прелистувачи	
Zero-phishing заштита	- заштита од непознати phishing страници во реално време - статичка и хеуристичка детекција на сомнителни елементи на веб страници коишто бараат приватни информации
Заштита на корпоративни креденцијали	Детекција на користење на корпоративни креденцијали на надворешни веб страници
URL филтрирање	- Екстензија за веб прелистувач која дозволува/блокира пристап до веб страници во реално време и потполна прегледност на HTTPS сообраќај
Безбедно пребарување	Интеграција со Интернет пребарувачи за автоматски филтер за потенцијално навредлива и несоодветна содржина
Sandboxing & Content Disarm & Reconstruction (CDR) за email и веб сообраќај	

Екстракција на закани	Отстранување на содржина што може да се злоупотреби, реконструкција на датотеки за елиминација на потенцијални злонамерни програми и достава на прочистена содржина до корисниците во неколку секунди.
Емулација на закани	- Можност за користење на sandbox за дектеција и блокирање на нови, непознати злонамерни програми и насочени напади коишто се наоѓаат во прилози во email, преземени датотеки, и URL до датотеки во email содржина - Заштита од различни типови на датотеки, вклучувајќи MS Office, PDF, Java, Flash, извршни датотеки и архиви - Откривање на закани скриени во SSL и TLS шифрирана комуникација
Endpoint Detection and Response (EDR)	
Собирање на форензички информации и автоматски извештаи	При детекција на злонамерен настан, автоматско покренување на форензичка анализа, и целата секвенца (историја) на нападот да биде презентирана како форензички извештај. Извештајот може да се искористи за спречување на идни напади и да се изврши проверка дека сите засегнати датотеки и процеси работат како што треба.
Мапирање на MITRE матрицата	MITRE ATT&CK конзола којашто дава прегледност во реално време на сите техники забележани од решението и мапирање на сите настани во MITRE тактики, техники и процедури.
Ловење на закани	Собирање на сите сирови и детектирани настани на крајниот уред, овозможувајќи напредни пребарувања, drill-down, и pivoting за проактивно ловење на закани и темелно истражување на инцидентите
Threat Intelligence	
Threat Feed	Комбинација на big data threat intelligence со напредни технологии на вештачка интелигенција коишто овозможуваат прецизна заштита од закани.
Управување со IOC	Додавање на Indicators of Compromise (IoC) за домени, IP адреси, URL, MD5 и SHA1 hash key коишто автоматски ќе бидат блокирани.

Поддржани оперативни системи	
Windows Workstation	Windows 11, 10, 8, and 7
Windows Server	Windows Server 2022, 2019, 2016, 2012, and 2008
MacOS	Sonoma (14), Ventura (13), Monterey (12), Big Sur (11), Catalina (10)
Ubuntu	Ubuntu (22.04-22.04.3, 20.04-20.04.6, 18.04-18.04.6, 16.04), Debian (9.12-11.8), RHEL (9.0, 9.3, 7.8-8.9), Alma Linux (9.0-9.3, 8.9), CentOS (7.8-8.5), Oracle Linux (7.9-8.8), Amazon Linux (2), SLES (12 SP5, 15 SP3), Open SUSE (15.3-15.5, 42.3), Fedora (34-39)
VDI & Terminal Server	VMware, Citrix, Terminal Server
Servers	SQL, Web Servers, DHCP Servers, Share Ppint (2010, 2016, 2013), Active Directory, Exchange, HyperV, DNS.
Централизирано управување преку on-prem конзола	
Централен уред за управување во форма на софтвер којшто може да се инсталира на следниве платформи	- KVM - MS Hyper-V - Vmware ESXi - Nutanix Acropolis Hypervisor - Azure Stack
Техничка поддршка и инсталлација	
Поддршка и ажурирање на софтвер	Техничка поддршка од производителот 24 x 7 за период од 12 месеци
	Пристап до база на знаење (Техничка документација) на производителот.
	Вклучено ажурирање на производот и дефинициите на сите видови закани во траење од 12 месеци.
Инсталација	Понудувачот мора да изврши инсталација на решението согласно најдобрите практики, интеграција со потребните системи, да напише техничка документација за начинот на извршената инсталација и конфигурација на системот.

Услови:

- Инсталација на антивирусен софтвер на сите клиенти и сервери. На серверите е поставен Active Directory и Фајл сервер, како и апликациски сервери и сервери со бази на податоци кои не смеат да имаат downtime, со што инсталацијата, доколку е потребно, би се имплементирала надвор од работно време. Носителот на набавката треба да ги предвиди сите подесувања (правила и исклучоци) на софтверот за да апликациите и сервисите кои ги користи Министерството за финансии продолжат непречено да функционираат;
- Обука на двајца вработени за користење и понатамошно одржување и поддршка за антивирусниот пакет;

Во моментов во инфраструктурата на Министерството е инсталиран и поставен антивирусен софтвер – **Kaspersky** на **650** работни станици и **75** сервери.Носителот на набавка на понуденото софтверско решение во соработка со ИТ лица од Министерството, е должен да го деинсталира тековниот софтвер од сите работни станици и сервери и да го инсталира новиот софтвер на работните станици и сервер. Деинсталацијата на старото антивирусно решение и инсталацијата на новото ќе се врши преку конзолата за централно управување на антивирусните решенија и со физички пристап на самите работни станици лоцирани во објектите на Министерството во Скопје. За останатите работни станици, во подрачните единици надвор од Скопје, инсталацијата ќе се врши далечински. По инсталација на софтверот носителот на набавката доставува детален извештај до Министерството за финансии;

- Бесплатни 'program upgrades' и 'program patches';
- Вклучена основна поддршка од страна на производителот на софтверот (право на надградби, закрпи, нови верзии и основна on-line техничка поддршка) за период од 1 (една) година;
- Носителот на набавката е должен во период од 1 (една) година да дава техничка подршка на on-site локација во случај на настанати проблеми (по пријава на договорниот орган). Времето на достапност на сервисот за техничка подршка треба да биде секој работен ден од 08-17 часот. Од страна на Министерството ќе биде овозможена и VPN врска за пристап доколку има потреба. Министерството располага со 6 локации во Скопје и 45 во државата. Доколку има потреба од интервенција на лице место на локацијата надвор од Скопје, технички лица од носителот на набавката во кординација со ИТ лица одат да интервенираат на локацијата;

- По склучување на договорот, Министерството ќе достави барање за инсталирање на антивирусниот софтвер и активација на лиценците по што носителот на набавка ќе биде должен да ја изврши инсталацијата во рок од 15 (петнаесет) работни денови од денот на добивање на барањето и обезбедување на технички предуслови од страна на Министерството.

Носителот на набавката е должен за решението (софтвер за антивирусна заштита на корисници / сервер) да вклучи и обезбеди: инсталација на истиот во времетраење од 15 (петнаесет) работни денови **ремоте обука за користење на системот на вработените во договорниот орган, како и минимум 1 (еден) ден ремоте во месецот за консултации во времетраење на претплатата, во согласност со техничките спецификации.**

НАПОМЕНА:
Доколку понудата отстапува од минималните барања содржани во оваа техничка спецификација, истата ќе се смета за неприфатлива и ќе биде отфрлена од страна на комисијата за јавни набавки.

- Економскиот оператор треба да е авторизиран од производителот за продажба и инсталација за типот на опрема која е предмет на оваа набавка на територијата на Р. Северна Македонија и Економскиот оператор го докажува со доставување (MAF-Manufacturer Authirisation Form) издадена од производителот.
- Недоставувањето е основ за отфрлање на понудата.

ПРИЛОГ 2

Техничка понуда

ТЕХНИЧКА ПОНУДА

II.1. Согласни сме да ви го обезбедиме предметот на набавка - софтвер за заштита на крајни корисници- next generatiron / сервер:___**Check Point Harmony Endpoint Advanced**_____**(Комерцијалното име на предметот на набавката да се наведе задолжително)** за период од 12 (дванаесет) месеци сметано од денот на целосната инсталација и ставање во употреба на истиот во се според барањата дефинирани во техничките спецификации кои се составен дел од тендерската документација.

II.2. **технички опис како ќе се постигнат бараните карактеристики барани од решението се следните:**

Р.Б	Карактеристики од решението		Опис како се постигнува: Checkpoint Harmony Endpoint Advanced
Контрола на пристап			
1	Огнен ѕид	Огнен ѕид за контрола на мрежниот сообраќај до и од крајните уреди, врз база на IP адреси домени, порти и и протоколи.	Firewall: Firewall rules accept or drop network traffic to and from Endpoints, based on IP addresses, Domains, Ports and Protocols. **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
2	Контрола на апликации	Контрола на мрежен пристап за одредени апликации. Правилата за контрола на апликации овозможуваат дозволување, блокирање или терминирање на апликации и процеси.	Application Control: Enable the option to restrict network access for specified applications. Application control rules define if to allow, block or terminate applications and processes. **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
3	Усогласеност на крајниот уред	Проверка дали уредот е во согласност со безбедносните правила на организацијата. Администраторот може да постави рестриктивни политики за неусогласените уреди.	Endpoint Compliance: The compliance component ensures Endpoint's compliance with the organization's security rules. Endpoints that do not comply show as "non-compliant" and the administrator can apply restrictive policies for them. **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
4	VPN за оддалечен пристап	VPN за оддалечен пристап којшто им овозможува на корисниците кои што работат од далечина безбедносен пристап и користење на апликации	Remote Access VPN: Virtual private network (VPN) enables users who are working remotely to securely access and use applications and data that reside in the corporate data center and headquarters, encrypting all traffic the users send and receive.

		што се наоѓаат во корпоративниот податочен центар. Целиот сообраќај што корисниците го примаат и праќаат треба да биде шифриран. Оваа функционалност треба да биде компатибилна со безбедносниот уред што го користи Договорниот орган.	**Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
Заштита од закани			
5	Заштита од ransomware	Постојано следење за специфично однесување на ransomware и идентификација на неодобрено шифрирање на датотеки без користење на дефиниции. Сите елементи на ransomware нападот се идентификувани преку форензичка анализа и се ставени во карантин - Враќање на податоци - шифрираните датотеки автоматски се враќаат од претходни snapshots - Intel TDT - имплементирана заштита на ниво на процесор со користење на Intel Threat Defense Technology.	Anti-Ransomware: Constantly monitors for ransomware specific behavior and identifies illegitimate file encryption, signature-less. Detect and quarantine all elements of a ransomware attack are identified by forensic analysis and then quarantined. Data Restoration - Encrypted files are automatically restored from snapshots to ensure full business continuity. Intel TDT – Implementing processor-level protection using Intel Threat Defense Technology. **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
6	Anti-Malware	Заштита од сите видови на злонамерни програми, од црви и тројанци до adware и keystroke loggers.	Anti -Malware: Protection from all kinds of malware threats, ranging from worms and Trojans to adware and keystroke loggers **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
7	Anti-Bot	Детекција и превенција на закани од ботови.	Anti-Bot: A bot is a malicious software that can invade and infect Endpoints with many infection methods. Harmony Endpoint Anti-Bot component detects and prevents all bots threats **Брошура**: harmony-endpoint-solution-

			brief-2024.pdf стр: 4
8	Anti-Exploit	Заштита од напади базирани на ранливости во легитимни апликации и исклучување на злоупотребениот процес при детекција на истото	Anti-Exploit: • Provides protection against exploit based attacks compromising legitimate applications, ensuring those vulnerabilities can't be leveraged. • Shuts down the exploited process upon detecting one, remediates the entire attack chain **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
9	Behavioral Guard	Адатаптивна детекција и блокирање на мутации на злонамерни програми врз основа на нивното однесување во реално време	Behavioral Guard: Adaptively detects and blocks malware mutations according to their real-time behavior. Identifies, classifies, and blocks malware mutations in real-time based on minimal process execution tree similarities. **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
10	Заштита на влезно/излезните портови на крајниот уред	Контрола за поврзување на периферни уреди (тастатура, монитор, bluetooth, печатачи, Smart Card, мрежни адаптери, глувчиња итн.	Port Protection: Protects sensitive information by requiring authorization for access to storage devices and other input/output devices. Port Protection protects the physical port when using peripheral devices. Peripheral devices are for example, keyboards, screens, blue tooth, Printers, Smart Card, network adapters, mice and so on. Брошура: harmony-endpoint-solution-brief-2024.pdf стр: 4 **Брошура**: CP_Harmony_Endpoint_AdminGuide.pdf стр: 400
Заштита на на Интернет прелистувачи			
11	Zero-phishing заштита	- заштита од непознати phishing страници во реално време - статичка и хеуристичка детекција на сомнителни елементи на веб страници	Zero-Phishing: Real-time protection from unknown zero-day phishing sites. Static and heuristic-based detection of suspicious elements across websites requesting private info **Брошура**: harmony-endpoint-solution-

		коишто бараат приватни информации	brief-2024.pdf стр: 4
12	Заштита на корпоративни креденцијали	Детекција на користење на корпоративни креденцијали на надворешни веб страници	Corporate Credential Protection: Detection of corporate credentials reuse on external sites. **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
13	URL филтрирање	- Екстензија за веб прелистувач која дозволува/блокира пристап до веб страници во реално време и потполна прегледност на HTTPS сообраќај	URL Filtering: URL Filtering **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
14	Безбедно пребарување	Интеграција со Интернет пребарувачи за автоматски филтер за потенцијално навредлива и несоодветна содржина	Safe Seach: Safe search is a feature added to search engines that acts as an automated filter for potentially offensive and inappropriate content **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
Sandboxing & Content Disarm & Reconstruction (CDR) за email и веб сообраќај			
15	Екстракција на закани	Отстранување на содржина што може да се злоупотреби, реконструкција на датотеки за елиминација на потенцијални злонамерни програми и достава на прочистена содржина до корисниците во неколку секунди.	Threat Extraction: Removes exploitable content, reconstructs files to eliminate potential threats and delivers sanitized content to users in a few seconds. **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
16	Емулација на закани	- Можност за користење на sandbox за дектеција и блокирање на нови, непознати злонамерни програми и насочени напади коишто се наоѓаат во прилози во email, преземени датотеки, и URL до датотеки во email содржина - Заштита од различни типови на датотеки, вклучувајќи MS Office, PDF,	Threat Emulation: Threat sandboxing capability to detect and block new, unknown malware and targeted attacks found in email attachments, downloaded files, and URLs to files within emails. Provides protection across widest range of file types, including Office, Adobe PDF, Java, Flash, executables, and archives, as well as multiple Windows OS environments. Uncovers threats hidden in SSL and TLS encrypted communications.

		Java, Flash, извршни датотеки и архиви - Откривање на закани скриени во SSL и TLS шифрирана комуникација	**Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
Endpoint Detection and Response (EDR)			
17	Собирање на форензички информации и автоматски извештаи	При детекција на злонамерен настан, автоматско покренување на форензичка анализа, и целата секвенца (историја) на нападот да биде презентирана како форензички извештај. Извештајот може да се искористи за спречување на идни напади и да се изврши проверка дека сите засегнати датотеки и процеси работат како што треба.	Forensics Collection & Automated Reports: On detection of a malicious event, Forensics analysis is automatically initiated, and the entire attack sequence is presented as a Forensics Report. By using the Forensics report, the user can prevent future attacks and to make sure that all affected files and processes work correctly. **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
18	Мапирање на MITRE матрицата	MITRE ATT&CK конзола којашто дава прегледност во реално време на сите техники забележани од решението и мапирање на сите настани во MITRE тактики, техники и процедури.	MITRE Mapping: The MITRE ATT&CK dashboard provides real-time visibility on all the techniques observed by Harmony Endpoint, it maps all events to MITRE tactics, Techniques and Procedure (TTPs). **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
19	Ловење на закани	Собирање на сите сирови и детектирани настани на крајниот уред, овозможувајќи напредни пребарувања, drill-down, и pivoting за проактивно ловење на закани и темелно истражување на инцидентите	Threat Hunting: Collection of all raw and detected events on the endpoint, enabling advanced queries, drill-down, and pivoting for proactive threat hunting and deep investigation of the incidents. **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
	Threat Intelligence		

20	Threat Feed	Комбинација на big data threat intelligence со напредни технологии на вештачка интелигенција коишто овозможуваат прецизна заштита од закани.	ThreatCloud: The brain behind Check Point Software's threat prevention power, combines big data threat intelligence with advanced AI technologies to provide accurate prevention to all Check ThreatCloud Point Software customers. **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
21	Управување со IOC	Додавање на Indicators of Compromise (IoC) за домени, IP адреси, URL, MD5 и SHA1 hash key коишто автоматски ќе бидат блокирани.	IOC Management: Indicator of Compromise (IoC) is an indicator to cyber security professionals about unusual activity or an attack. Harmony Endpoint allows you to add IoCs for domains, IP addresses, URLs, MD5 Hash keys and SHA1 Hash keys that will automatically block. **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 4
Поддржани оперативни системи			
22	Windows Workstation	Windows 11, 10, 8, and 7	Operating Systems: Windows Workstation – 11, 10, 8, and 7 **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 3
23	Windows Server	Windows Server 2022, 2019, 2016, 2012, and 2008	Operating Systens: Windows Server – 2022, 2019, 2016, 2012, and 2008 **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 3
24	MacOS	Sonoma (14), Ventura (13), Monterey (12), Big Sur (11), Catalina (10)	Operating Systens: MacOS –Sonoma (14), Ventura (13), Monterey (12), Big Sur (11), Catalina (10) **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 3
25	Ubuntu	Ubuntu (22.04-22.04.3, 20.04-20.04.6, 18.04-18.04.6, 16.04), Debian (9.12-11.8), RHEL (9.0, 9.3, 7.8-8.9), Alma Linux (9.0-9.3, 8.9), CentOS (7.8-8.5), Oracle Linux (7.9-8.8), Amazon Linux (2), SLES (12 SP5, 15 SP3), Open SUSE (15.3-15.5, 42.3), Fedora (34-39)	Operating Systems: Linux – Ubuntu (22.04-22.04.3, 20.04-20.04.6, 18.04-18.04.6, 16.04), Debian (9.12-11.8), RHEL (9.0- 9.3, 7.8-8.9), Alma Linux (9.0-9.3, 8.9), CentOS (7.8-8.5), Oracle Linux (7.9-8.8), Amazon Linux (2), SLES (12 SP5, 15 SP3), Open SUSE (15.3-15.5, 42.3), Fedora (34-39) **Брошура**: harmony-endpoint-solution-

			brief-2024.pdf стр: 3
26	VDI & Terminal Server	VMware, Citrix, Terminal Server	Operating Systems: VDI & Terminal Server – VMware, Citrix, Terminal Server **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 3
27	Servers	SQL, Web Servers, DHCP Servers, Share Ppint (2010, 2016, 2013), Active Directory, Exchange, HyperV, DNS.	Operating Systems: Servers – SQL, Web Servers, DHCP Servers, Share Ppint (2010, 2016, 2013), Active Directory, Exchange, HyperV, DNS **Брошура**: harmony-endpoint-solution-brief-2024.pdf стр: 3
Централизирано управување преку on-prem конзола			
28	Централен уред за управување во форма на софтвер којшто може да се инсталира на следниве платформи	- KVM - MS Hyper-V - Vmware ESXi - Nutanix Acropolis Hypervisor - Azure Stack	Centralized Management: Compatible Hardware Archive - Check Point Software
Техничка поддршка и инсталлација			
29	Поддршка и ажурирање на софтвер	Техничка поддршка од производителот 24 x 7 за период од 12 месеци	Direct Premium For 1Y; Service and Support, Issues Opened with Techincal Support Engineer. **Брошура**: checkpoint-support-datasheet.pdf стр:2
		Пристап до база на знаење (Техничка документација) на производителот.	SecureKnowledge Access: Expert **Брошура**: checkpoint-support-datasheet.pdf стр:2
		Вклучено ажурирање на производот и дефинициите на сите видови закани во траење од 12 месеци.	Every level of your support program includes critical software bug fixes and automatic updates to ensure continuing system maintenance and proper functionality for all your Check Point products; Hot Fixes/ Service Packs, Major Upgrades/ Enhancements **Брошура**: checkpoint-support-datasheet.pdf стр:2

30	Инсталација	Понудувачот мора да изврши инсталација на решението согласно најдобрите практики, интеграција со потребните системи, да напише техничка документација за начинот на извршената инсталација и конфигурација на системот.	Инсталација на решението согласно најдобрите практики, интеграција со потребните системи. Техничка документација за начинот на извршената инсталација и конфигурација на системот.

Колоната Опис како се постигнува задолжително се потполнува, а понудувачот треба да достави и линкови до оригинални брошури или презентации поврзани со понуденото решение.
Доколку не се пополнат сите празни места и не се достават линкови до оригинални брошури или презентации поврзани со понуденото решение понудата ќе биде отфрлена.

НАПОМЕНА: **Економскиот оператор ја потпишува со валиден дигитален сертификат и прикачува техничката понуда во моментот на поднесување на понудата како дел од целокупната документација.**
Недоставувањето на техничка понуда е основ за отфрлање на понудата.