Обґрунтування технічних та якісних характеристик предмета закупівлі, його очікуваної вартості та/або розміру бюджетного призначення відповідно до пункту 4[1] постанови Кабінету Міністрів України від 11.10.2016 року №710 «Про ефективне використання коштів» (зі змінами)

1. Замовник:	
Назва замовника	Національний фонд досліджень України
Код за ЄДРПОУ	42734019
Місцезнаходження	01001, м. Київ, вул. Бориса Грінченка, 1
2. Номер закупівлі в електронній системі Prozorro	UA-2025-11-04-015640-a
3. Предмет закупівлі:	
Вид предмета закупівлі	Відкриті торги з особливостями
Конкретна назва предмета закупівлі	Послуги з постачання, встановлення і налаштування програмної продукції Check Point
Коди та назви відповідних класифікаторів предмета закупівлі і частин предмета закупівлі (лотів) (за наявності)	ДК 021:2015: 72260000-5 — Послуги, пов’язані з програмним забезпеченням
4. Обґрунтування очікуваної вартості предмета закупівлі, розмір бюджетного призначення	Очікувану вартість предмету закупівлі визначено відповідно до Наказу Міністерства розвитку економіки, торгівлі та сільського господарства України № 275 від 18.02.2020 «Про затвердження примірної методики визначення очікуваної вартості предмета закупівлі» (далі – Методика). Метод, що застосовано відповідно до Методики: розрахунок очікуваної вартості товарів/послуг на підставі отриманих комерційних пропозицій. Розмір бюджетного призначення – 808 300,00 грн (вісімсот вісім тисяч триста гривень 00 копійок) з ПДВ
5. Строк поставки товарів (надання послуг, виконання робіт)	до 15 грудня 2025 року
6. Обґрунтування технічних та якісних характеристик предмета закупівлі	**<u>Загальні вимоги:</u>** Виробник Програмної продукції повинен бути представлений в Україні в вигляді офіційного представництва, що повинно бути відображено на офіційному сайті виробника. Виробник повинен мати мережу офіційних партнерів в Україні, перелік яких повинен бути наведений на спеціалізованому офіційному веб-ресурсі виробника. Виробник повинен мати щонайменше два офіційних діючих дистриб’ютора в Україні, перелік яких повинен бути наведений на спеціалізованому офіційному веб-ресурсі виробника. Виконавець повинен надати Замовнику авторизаційний лист (форму) від виробника або його офіційного представника в Україні на право постачати в Україні Програмну продукцію. Послуга з постачання Програмної продукції включає право надання Замовнику доступу на отримання змін, оновлень, додатків, доповнень, підписок терміном не менше 36 (тридцяти шести) місяців. **<u>Вимоги до послуг, що надаються:</u>** Послуги, що надаються Учасником повинні включати постачання, встановлення і налаштування програмної продукції фахівцями Учасника, що мають включати наступні етапи:

	1. Інсталяція та первинна конфігурація обладнання: встановлення та налаштування у відповідності до технічних вимог Замовника. 2. Тестування функціональності: перевірка системи на відповідність необхідним вимогам безпеки та продуктивності. 3. Технічна підтримка на період інтеграції: супровід процесу введення в експлуатацію. 4. Постійна технічна підтримка: забезпечення обслуговування протягом усього часу використання обладнання. 5. Гарантійне обслуговування 24x7x365 – 24 (двадцять чотири) години на добу, 7 (сім) днів на тиждень, 365 (триста шістдесят п'ять) днів на рік, включаючи святкові, вихідні та неробочі дні. 6. Розширені технічні консультації з питань конфігурації та функціонування Програмної продукції по телефону _____ (з можливостю зв'язку з технічними спеціалістами по місцевому телефону без використання послуг міжнародного телефонного зв'язку) та електронній пошті _____. **<u>Технічні вимоги до Програмної продукції:</u>** **Програмна продукція Check Point Smart-1 Cloud to manage 5 SMB (Gaia Embedded) gateways with up to 3 GB daily logs 3 months retention, including SmartEvent blade** 1. Наявність графічного інтерфейсу (GUI) для керування. Графічний інтерфейс (GUI) повинен дозволяти відслідковувати поточний статус міжмережевих екранів та основних його параметрів (щонайменше: версію програмного забезпечення, відсоток використання CPU, відсоток використання пам'яті, перелік розділів жорсткого(-их) диску(-ів) та відсоток використання вільного місця на цих розділах). 2. Наявність функціоналу підтримки облікових записів адміністраторів на основі ролей. 3. Наявність функціоналу централізованого розповсюдження та застосування нових версій програмного забезпечення з метою оновлення як міжмережевих екранів так й серверів керування міжмережевими екранами. 4. Наявність функціоналу централізованого застосування та оновлення ліцензій що активують відповідний функціонал міжмережевих екранів. 5. Наявність функціоналу застосування правил безпеки на вибраних міжмережевих екранах. 6. Наявність функціоналу збору та збереження подій, що відбуваються на міжмережевих екранах, перегляд таких подій. 7. Наявність функціоналу аналізу збережених подій що відбуваються на всіх міжмережевих екранах та подальша їх кореляції між собою. 8. Наявність функціоналу повідомлень адміністраторів (електронним листом, завантаження даних на інші системі тощо) в разі виявлення загроз та подій, що базуються на раніше заданих умовах. 9. Наявність функціоналу аналізу стану безпеки організації що дає повне уявлення про стан інформаційної безпеки в цілому та небажані процеси, які проходять в інфраструктурі. 10. Наявність функціоналу керування ризиками інформаційної безпеки та перевірка на відповідність регуляторним вимогам (PCI DSS, HIPPA, GDPR тощо), що пов'язані з

	налаштуваннями міжмережевих екранів, та надання рекомендацій щодо їх усунення відповідно до рекомендацій виробника та світових стандартів. 11. Механізм керування міжмережевими екранами з спеціалізованої командної строки (CLI), в тому числі – з метою доступу до експертних налаштувань та пошуку неполадок (виявлення та локалізації проблем). 12. Механізм перегляду консолідованої звітності що дозволяє переглядати в графічній консолі (GUI) щонайменше таку інформацію: Кількість з'єднань заблокованих певним правилом безпеки. Топ-джерела заблокованих з'єднань, їхні призначення та сервіси. Топ-правила (політики безпеки), що використовуються відпрацювали. Топ-атаки, виявлені на периметрі екранів, їхні джерела та призначення. Загальна кількість політик безпеки екранів. Найбільша активність по кожному користувачеві, з можливістю деталізації щодо найпопулярніших відвідуваних сайтів. Топ-користувачів з найдовшою тривалістю шифрованих сесій (VPN-з'єднань). 13. Забезпечення безпечного керування всіма пристроями, а саме: Наявність ролей для облікових записів адміністраторів. Шифровані комунікації між консолю \ сервісом централізованого керування та міжмережевими екранами. Механізм лічильників спрацювань правил політики інформаційної безпеки. Механізм пошуку по журналам подій (наприклад для визначення, чи містить той чи інший мережевий об'єкт конкретну IP-адресу чи її частину). Механізм сегментації політик безпеки з використанням міток або заголовків відповідного розділу налаштувань політик для більш зручної організації та візуалізації політики безпеки. Механізм верифікації політики безпеки, що перевіряє створену політику безпеки до її застосування на міжмережевому(-их) екрані(-ах). Механізм централізованого розповсюдження та встановлення нових версій програмного забезпечення на міжмережеві екрани з системи централізованого керування. Інструментарій централізованого обліку та керування ліцензіями всіх міжмережевих екранів. Механізм реалізації ієрархічної системи керування на основі структур доменів (multi-domain management) та підтримка концепції розповсюдження глобальних політик безпеки на всі такі домени одночасно. Графічний інтерфейс (GUI) сервера централізованого керування повинен мати однакові можливості як для архітектури з одним доменом, так й для архітектури в вигляді мульті доменного середовища. Журнал перегляду подій з можливістю висвітлювання всіх наявних подій безпеки в одній віконній області з метою ефективного виявлення проблематики. Журнал перегляду подій з можливістю створення власних фільтрів на базі попередньо визначених об'єктів (хостів, мереж, групи користувачів тощо), в тому числі - для повторного використання в майбутньому

	Журнал перегляду подій з можливістю створення та збереження довільних фільтрів для повторного (подальшого) використання в майбутньому. Механізм пошуку по заданому мережевому об'єкту в усіх політиках та налаштуваннях одночасно. Наявність API для роботи з ним з будь-якими визначеними користувачем клієнтськими застосунками. Механізм оповіщення адміністраторів щодо можливої неправильної конфігурації. 14. Ведення журналів подій для всіх міжмережевих екранів, а саме: Централізоване протоколювання всіх подій з можливістю (в разі необхідності) встановлення окремих (виділених) систем протоколювання для проміжного збору журналів подій (з подальших їх переглядом в консолі сервера централізованого керування міжмережевими екранами). Механізм індексації журналів подій безпеки та індексованого швидкого пошуку будь-яких подій безпеки. Механізм автоматичного захоплення мережевих пакетів для подій пов’язаних безпосередньо з системою запобігання вторгненням (IPS) з метою забезпечення їх більш поглибленого подальшого аналізу (для Першого та Другого кластера). Журнали подій щодо активності адміністраторів сервера централізованого керування міжмережевими екранами. Окремі журнали подій щодо функціонуванням модулів захистів (IPS, AV, Application Control, URL і тому подібне). Механізм швидкого перемикання (в один клік миші) між подією в журналі подій до відповідного правила політики безпеки (до якого відноситься дана подія). Механізм що дозволяє застосування для будь-якого правила політики безпеки наступні дії, щонайменше: протоколювання події (log), оповіщення адміністратора (alert), включаючи оповіщення електронним листом, запуск скрипту (завчасно визначеного адміністратором сервера централізованого керування міжмережевими екранами). Механізм динамічного блокувати активного мережевого з'єднання за допомогою графічного інтерфейсу без необхідності вносити зміни безпосередньо в політику безпеки. Механізм експорту журналу подій в сторонні системи аналізу інцидентів (SIEM). Механізм задання асоціювання ім'я користувача та назви комп'ютера щодо події безпеки (для кожного запису в журналі подій). Механізм перегляду усіх VPN-тунелів, (як site-to-site VPN, так й client-to-site VPN) з функцією виявлення проблеми щодо функціонування тунелів та подальшим занесенням таких подій до журналу(-ів) подій та повідомленням адміністратора. Механізм встановлення лімітів (обмежень) щодо певних параметрів продуктивності компонентів (модулів захисту) екранів, при досягнення яких повинні відбуватися задані дії, щонайменше такі як: протоколювання, надсилання повідомлення. Доступність графічних звітів з деталізацією для об’єктів, що проходили емуляцію в спеціальному середовищі («пісочниці» \ sandbox або аналог), які надають щонайменше таку інформацію (для об’єктів що визнані небезпечними): звідки прийшов заражений об’єкт (файл, мережа, електронна пошта тощо), класифікація вірусу, поведінка віруса (перелік його дій, в тому числі – перелік технік та технологій відповідно до матриці атак MITRE ATT&CK).

	Інструментарій кореляції подій безпеки, а також можливість підключення зовнішніх пристроїв (сервісів) від сторонніх виробників для «насичення» даними для такої кореляції. Механізм створювання фільтрів перегляду подій, що обмежують множину відображення певними характеристиками подій, щонайменше такими як: заданий модуль захисту, IP-адреса джерела, IP-адреса призначення, класифікація події, рівень критичності події, країна джерела, країна призначення. Механізм експорту події в вигляді звіту з наявного журналу подій у зовнішній(-і) файл(-и) в різних форматах, такі як PDF, HTML, CSV, MHT тощо. Механізм створення подій, що пов'язані з входом (логіном) адміністратора сервера централізованого керування міжмережевими екранами до сервера у нетипові (наприклад, не робочі) години доби. Механізм створення подій, що пов'язані з спробами підбору облікових даних адміністраторів сервера централізованого керування міжмережевими екранами. Наявність автоматичних годинних, денних, тижневих та місячні звітів та можливість створити такі звіти за заданим розкладом. **Програмна продукція повинна відповідати наступним показникам максимальної продуктивності, щонайменше:** 1. Максимальна кількість міжмережевих екранів з різними політиками, котрими одночасно може керувати менеджмент – *не менш ніж **5** (п'ять).* 2. Час зберігання журналів подій – *не менш ніж **3 міс** (три місяця).* 3. Об'єм зберігання журналів подій за день (24 години) – *не менш ніж **3Гбайт** (три гігабайт).* **Програмна продукція Check Point Harmony Endpoint Advanced – Including Sandboxing, Web Protection, Attack Investigation, Threat Prevetion, Access Control and Threat Intelligence, включаючи технічну підтримку рівня Standart Collaborative Enterprise (для 80 кінцевих точок)** 1. Наявність функціоналу локального брандмауера (Firewall). 2. Наявність функціоналу віддаленого безпечного підключення користувачів до інфраструктури Замовника (VPN з'єднання типу Site to Client). 3. Наявність функціоналу контролю доступу користувачів до веб-ресурсів (URL Filtering або аналог). 4. Наявність функціоналу аналізу об'єктів (файлів), що перевіряються екраном, за допомогою сигнатурного аналізу антивірусу (Antivirus або аналог). 5. Наявність функціоналу аналізу об'єктів (файлів), що перевіряються екраном, за допомогою евристичного аналізу та техніками машинного аналізу та штучного інтелекту. 6. Наявність функціоналу аналізу об'єктів (файлів, посилань, листів тощо), що перевіряються мережевим екраном, за допомогою емуляції в окремому апаратному або хмарному середовищі («пісочниці» \ Sandbox або аналог) з метою виявлення раніше невідомих загроз (0day або аналог). 7. Наявність функціоналу видалення потенційно активного (небезпечного) вмісту в файлах Office (doc, xlx, ppt тощо) та файлах формату PDF.

	8. Наявність функціоналу конвертації файлів Office (doc, xlx, ppt тощо) в формат PDF з видаленням потенційно активного (небезпечного) вмісту. 9. Наявність функціоналу запобіганню з'єднань з командними центрами зловмисників та сайтами зловмисників (що використовуються з метою завантаження шкідливих додатків), а також функціонал виявлення мережевих з'єднань, характерних для комунікацій ботів та бот-мереж (Anti-Bot або аналог). 10. Наявність функціоналу блокування програмних застосунків (Application Control або аналог), в тому числі – можливість блокування тільки мережевих комунікаій. 11. Наявність функціоналу блокування дій вірусів-шифрувальників з можливістю відновлення даних що було зашифровано в результаті таких дій (Anti-Ransomware або аналог) 12. Наявність функціоналу детального пошуку подій за індикаторами компрометації (IP, назва ПК або користувача, хеш-суми процесів або програмних застосунків тощо) що відбувалися на кінцевих робочих точках (Threat Hunting або аналог). 13. Наявність функціоналу розслідування (forensic та EDR або аналог) виявленої та блокованої атаки на кінцеву робочу точку з можливістю побудови детальної карти взаємодій компонентів операційної системи, таких як послідовність запущених процесів, спосіб проникнення вірусу, змінені гілки реєстру ОС, IP-адреса звідки була здійснена атака, методи які використовував зловмисник тощо. 14. Наявність графічного інтерфейсу (GUI) для керування захистом на всіх кінцевих точках та безпосередньо самим сервісом централізованого керування. 15. Наявність функціоналу підтримки облікових записів адміністраторів на основі ролей. 16. Наявність функціоналу централізованого розповсюдження та застосування нових версій програмного забезпечення захисту кінцевих точок. 17. Наявність функціоналу централізованого застосування та оновлення ліцензій що активують (або деактивують) відповідний функціонал захисту кінцевих точок. 18. Наявність функціоналу застосування правил безпеки на вибраних кінцевих точках або груп користувачів. 19. Наявність функціоналу збору та збереження подій, що відбуваються на кінцевих точках, перегляд таких подій. 20. Наявність функціоналу повідомлень адміністраторів (електронним листом, завантаження даних на інші системі тощо) в разі виявлення загроз та подій, що базуються на раніше заданих умовах. 21. Наявність функціоналу аналізу стану безпеки організації що дає повне уявлення про стан інформаційної безпеки на рівні кінцевих точках. 22. Наявність функціоналу інтеграції з каталогами користувачів Замовника (LDAP, AD тощо) з метою отримання різноманітних даних про користувачів (належність до групи, телефон, підрозділ тощо) та застосування правил до груп або окремих користувачів. 23. Наявність функціоналу захисту за допомогою вбудованого антивірусного(-их) механізму(-ів), механізмів виявлення бот-активності та механізмів виявлення мережевих атак, а саме: Наявність багаторівневого механізму детектування, котрий містить такі технології як сигнатурний аналіз та репутаційна база об'єктів (хеш-суми, IP-адрес, URL та DNS-адреси тощо), а також

	аналізатор мережевих з'єднань, що виявляє ознаки, характерні для комунікацій ботів. Можливість виявлення та блокування вірусів-шифрувальників за допомогою статичного та динамічного аналізу. Можливість автоматичного відновлення даних користувачів після успішних атак в разі роботи вірусів-шифрувальників на кінцевій станції. Можливість виявлення та блокування об'єктів, що використовують фішингові атаки, в тому числі – об'єкти у вигляді веб-сторінок під час роботи користувачів в мережі Інтернет. Обов'язкова наявність функціоналу блокування полів вводу даних (логін, пароль, e-mail, номер кредитної карти тощо) без можливості вводу будь-яких даних в такі поля до результатів такої перевірки. Можливість пошуку загроз (вірусів) в архівах (щонайменше в архівах форматів (ZIP, 7z, RAR, CAB, TAR, BZ2). Можливість захисту від використання експлойтів що орієнтовані на програмні додатки (щонайменше в Office, Adobe) та плагіни в браузерах (Java, Flash та інші). Можливість виявлення та запобігання вихідних комунікацій кінцевої робочої точки з зовнішніми небезпечними джерелами, наприклад, C&C (Command Center) зловмисників. Можливість детектування та запобігання наступним загрозам: нелегітимне використання протоколів, комунікація зловмисного програмного забезпечення з центрами зловмисників, спроби створення тунелів та загальні атаки без попередньо визначених (відомих) сигнатур. Можливість виявлення за запобігання «горизонтальним» комунікаціям (через внутрішні мережі Замовника) шкідливим додаткам та процесам, в тому числі таким, що використовують недоліки («дірки»)вразливості операційних систем та їх компонентів (протоколів, вразливостей додатків тощо). 24. Контроль мережевого трафіку (в тому числі, при застосуванні протоколів HTTPS), а саме: Наявність механізму URL-фільтрації, в тому числі з можливістю блокування доступу, на рівні кожної кінцевої точки за конкретно заданими доменами. Наявність механізму URL-фільтрації на рівні кожної кінцевої точки, в тому числі з можливістю блокування доступу, за заданими категоріями сайтів (соціальні мережі, реклама тощо). Наявність механізму відстеження використання корпоративних паролів на сторонніх веб-ресурсах на рівні кожної кінцевої точки. Наявність механізму створення правил фільтрації, що містить декілька URL-категорій. Наявність механізму створення правил що можуть застосовуватися до користувачів або групи користувачів або їх комбінації. База даних контролю програмних додатків та URL-фільтрації має оновлюватися через хмарний сервіс виробника. Можливість персоналізації інформаційних сторінок («заглушок») для інформування користувача про причини заборони доступу до бажаного веб-ресурсу (веб-сторінки). 25. Перевірка об'єктів за допомогою спеціального зовнішнього середовища емуляції («пісочниці») для раніше невідомого шкідливого коду, а також видалення потенційно небезпечного коду з файлів: Наявність механізму емуляції для об'єктів що надсилаються (скачуються або передаються) з веб-ресурсів що розташовані в мережі

	інтернет (незалежно від типу протоколу – HTTP, FTP, SMB тощо), а також запускаються безпосередньо з файлової системи операційної системи або змінних носіїв. Перевірка в спеціальному середовищі емуляції («пісочниця») має бути інтегрована в єдину багаторівневу архітектуру запобігання кіберзагрозам - разом з іншими модулями захисту та механізмами перевірки Виробника. Перевірка в спеціальному середовищі емуляції («пісочниця») може проводитися як локально так і за допомогою надсилання об'єкту перевірки до хмарного сервісу Виробника. Тривалість такої перевірки не повинна перевищувати 7 (сім) хвилин. Можливість емуляції бінарних файлів, архівних файли, документів Office та PDF, Java, Flash, щонайменше: com, exe, dll, 7z, cab, csv, doc, docm, docx, dot, dotm, dotx, exe, jar, pdf, potx, pps, ppsm, ppsx, ppt, pptm, pptx, rar, rtf, scr, swf, tar, xla, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, zip, pif, pif, com, gz, bz2, tgz, ISO, js, cpl, vbs, jse, vba, vbe, wsf, wsh. Можливість емуляції, в тому числі, файлів що передаються наступними протоколами: HTTP, HTTPS, FTP, SMTP, CIFS (SMB), SMTP TLS. Наявність механізму емуляції в різних операційних системах, щонайменше: Windows XP, Windows 7, Windows 8, Windows 10, Windows 11. Наявність механізму, що запобігає потраплянню в корпоративну мережу файлів, що проходять емуляцію, до отримання результатів такої емуляції (функціонал Prevent). Можливість виконувати статичну фільтрацію (за сигнатурами, поведінковим контролем, репутацією тощо) на стадії, що передує емуляції. Можливість емуляції файлів, розмір котрих перевищує 20 MB (для будь-якого з типів файлів, що підтримуються). Наявність технології машинного навчання. Можливість виявлення технік експлуатації, що використовують складні техніки типу return oriented programming (ROP) та інші техніки (наприклад, ескалацію привілеїв) шляхом відслідковування виконання інструкцій на рівні центрального процесора (а не на рівні процедур та системних дій на рівні операційної системи). Наявність механізму, що дозволяє проводити емуляцію (та вилучати) файли, що вмонтовані (вкладені) в документи. Наявність механізмів, що виявляє та блокує наступні спроби обходу середовища емуляції («пісочниці»): - спроби шкідливого коду блокувати запуск, якщо він виявляє віртуальне середовище; - спроби затримки запуску безпосередньо шкідливим кодом; - спроби виключення або перезапуску операційної системи емуляції та спроби запуску шкідливого коду у такі моменти; - спроби інтерактивної взаємодії з користувачем, в тому числі – спроби виявлення присутності людини (середовища емуляції має відтворювати діяльність реального користувача як то клацання миші, натискання клавіш клавіатури і тому подібне); - спроби підробок піктограм програмних додатків з метою введення в оману користувача. Наявність механізму, що протидіє загрозам шляхом вилучення потенційно можливого шкідливого вмісту (такого як активний код, URL-посилання, інші вкладені файли та вбудовані об'єкти, скрипти тощо) з файлів сімейства Office та файлів PDF, що завантажуються через браузер, навіть якщо такі файли ще не пройшли перевірку в

	середовищі емуляції. Наявність функціоналу отримання оригінального файлу, в разі якщо після емуляції він визнаний безпечним. Наявність механізму, що протидіє загрозам шляхом конвертації файлів, що завантажуються через браузер, сімейства Office з потенційно можливим шкідливим вмістом (таким як активний код, URL-посилання, інші вкладені файли та вбудовані об'єкти, скрипти тощо) в формат PDF з одночасним вилученням такого вмісту, навіть якщо такі файли ще не пройшли перевірку в середовищі емуляції. Наявність функціоналу отримання оригінального файлу, в разі якщо після емуляції він визнаний безпечним. 26. Наявність механізму поведінкового контролю додатків та процесів що запускаються та виконуються на кінцевій точці з можливістю реагування (в тому числі – блокування) шкідливих дій 27. Перевірка об’єктів операційної системи (файлова система, процеси, ОЗП) на предмет шкідливого програмного коду за заданим адміністратором розкладом. 28. Автоматичне реагування на шкідливі дії (віруси, атаки через мережу, скрипти тощо) як з заданими реакціями на такі дії (такі як: видалення шкідливого об’єкту, переміщення шкідливого об’єкту до спеціального середовища карантину, в тому числі – спеціально задану папку або зовнішній сервер, журналювання події тощо), так і на основі штучного інтелекту та машинного аналізу. 29. Обов’язкова наявність автономного механізму збереження подій (на кожній кінцевій точці), що відбувалися під час виконання шкідливих дій з функціоналом побудови детальної карти (схеми) з переліком всіх об’єктів та їх взаємовідносинами, що використовувалися при таких шкідливих діях. 30. Контроль та можливість блокування програмних додатків кінцевої робочої точки, в тому числі – змінних, з наступним функціоналом: Блокування запуску додатку за заданими критеріями (сертифікатом виробника програмного додатку, назвою файлу, хеш-сумою тощо). Дозвіл запуску але блокування мережевих комунікацій додатку за заданими критеріями (сертифікатом виробника програмного додатку, назвою файлу, хеш-сумою тощо). Можливість сканування кінцевих точок на предмет встановлених додатків з подальшим доданням їх до правил безпеки. 31. Перевірка кінцевої точки на предмет заданих стандартів (параметрів) організації, що дозволяє реалізувати перевірку наступних параметрів: Наявність актуальної сигнатурної бази антивірусного захисту. Наявність необхідних (заданих) оновлень операційної системи. Наявність необхідного (заданого) переліку програмних додатків. Перевірка параметрів операційної системи (гілки реєстру, версія, бібліотеки тощо). 32. Наявність функціоналу з можливістю задання реакцій на невідповідність заданими критеріям (стандартам) щонайменше: інформування користувача, інформування адміністратора, запуск необхідного команди, запуск скрипту. 33. Наявність функціоналу заборони відключення модулів захисту безпосередньо користувачем. 34. Застосування різних політик безпеки в залежності від місцезнаходження кінцевої точки (її доступності з ПЗ або веб-сервісу для централізоване керування або недоступності).

	35. **Програмна продукція повинна відповідати наступним показникам працездатності:** 1. Повинна забезпечуватися працездатність компонентів на кінцевих точках, що відповідають наступним фізичним характеристикам: - не гірше ніж x86/64-based процесор з частотою не менш 2 ГГц; - не менш ніж 4 ГБ ОЗП; - не менш ніж 6 ГБ на жорсткому диску. 2. Повинна забезпечуватися працездатність компонентів на кінцевих точках, на яких встановлена одна з наступних операційних систем: - Microsoft Windows версій 7 SP1, 8.1 Update 1, 10 (LTSC, 19H1 , 19H2, 20H1, 20H2, 21H1, 21H2, 21H2, 22H2), 11 (21H2, 22H2, 23H2); - Microsoft Windows Server версій 2008 R2 32/64-bit, 2012 64-bit, 2012 R2 64-bit, 2016 64-bit, 2019 64-bit, 2022 64-bit; - macOS версій Catalina (10.15), Big Sur (11), Monterey (12), Ventura (13), Sonoma (14). **Обґрунтування**: посилання на конкретну торгівельну марку пов'язане із запланованою закупівлею міжмережевого екрану Check Point 1600 Appliance з підпискою SandBlast та необхідністю (з метою) створення єдиної платформи від єдиного виробника Check Point, що значно спростить адміністрування та задовільний повний спектр потреб Замовника в інформаційні безпеці, розширену функціональність, сучасну підтримку, надійний і ефективний захист ІТ-інфраструктури.