|  |
| --- |
| Назва закупівлі: **надання Ліцензії на використання програмної продукції ESET Secure Business та ESET Secure Authentication**Класифікатор та його відповідний код: **ДК 021:2015: 48760000-3: Пакети програмного забезпечення для захисту від вірусів**Процедура закупівлі: **Відкриті торги**Очікувана вартість: **400 000,00 UAH з ПДВ**Дата оприлюднення: **25 травня 2022 року**Детальна інформація за посиланням: <https://prozorro.gov.ua/tender/UA-2022-05-25-004904-a>Інформація про необхідні технічні, якісні та кількісні характеристики предмета закупівлі |

**надання Ліцензії на використання програмної продукції ESET Secure Business та ESET Secure Authentication**

**(ДК 021:2015 - 48760000-3 Пакети програмного забезпечення для захисту від вірусів)**

|  |  |  |
| --- | --- | --- |
| № з/п | Найменування Ліцензії \* | Кількість шт. |
|  | Програмна продукція 'ESET Secure Business' (G). На 1 рік. Поновлення. Для захисту 550 об'єктів.  | 1 |
|  | Програмна продукція 'ESET Secure Authentication' (B11). На 1 рік. Пільгова. Для захисту 10 об'єктів. | 1 |

\*У разі якщо присутнє посилання на конкретну торговельну марку чи фірму, патент, конструкцію, вважати це «або еквівалент».

* **Вимоги до технічної підтримки**

 Запропонована антивірусна ПП повинна мати авторизований виробником центр технічної підтримки на території України, який має забезпечувати надання технічної підтримки користувачам відповідно до наступних вимог:

- обслуговування 24/7/365 - 24 години на добу, 7 днів на тиждень, 365 днів на рік, включаючи святкові, вихідні та неробочі дні;

- розширені технічні консультації з питань конфігурації та функціонування антивірусної ПП по телефону (з можливостю зв’язку з технічними спеціалістами по місцевому телефону без використання послуг міжнародного телефонного зв’язку) та електронній пошті;

- виїзд інженера на місце розташування Замовника у випадках збоїв роботи антивірусної ПП.

* **Вимоги до рішення для захисту робочих станцій**
* Підтримка ОС: Microsoft Windows Vista (Professional або вище); Microsoft Windows 7 (Professional або вище); Microsoft Windows 8 (Professional або вище); Microsoft Windows 8.1 (Professional або вище); Microsoft Windows 10; Microsoft Windows Server 2012R2, 2012, 2008R2, 2008, Microsoft Win. Server Core 2012R2, 2012, 2008R2, 2008 Core; Linux Kernel версії 2.6.x та вище.
* Надання захисту від: вірусів, троянського ПЗ, рекламного ПЗ, фішингу, а також шпигунського ПЗ.
* Надання захисту від шкідливого ПЗ - певного шкідливого коду, який додається на початок або кінець коду наявних файлів на комп’ютері. Виявлення шкідливого ПЗ повинно здійснюватися ядром виявлення в поєднанні з компонентом машинного навчання.
* Надання захисту від потенційно небажаних програм, яких не можна однозначно віднести до шкідливого ПЗ за аналогією з такими безумовно шкідливими програмами, як віруси або трояни, але ці програми можуть інсталювати додаткове небажане ПЗ, змінювати поведінку або налаштування цифрового пристрою, а також виконувати неочікувані для користувача дії або не підтверджені ним.
* Надання захисту від потенційно небезпечних програми - комерційного легального ПЗ, що може використовуватися для зловмисних цілей, таких як несанкціонований віддалений доступ, викрадення або злам паролів, клавіатурні шпигуни тощо.
* Надання захисту від підозрілих програм – програм, які стиснуті пакувальниками або протекторами, що часто використовують зловмисники за для того, щоб запобігти виявленню шкідливого програмного забезпечення.
* Надання захисту від небезпечних програм руткітів, які надають зловмисникам з Інтернету необмежений доступ до системи, водночас приховуючи свою присутність в операційній системі.
* Можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування.
* Можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення в роботі або впливати на продуктивність системи.
* Можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання в процес роботи ОС.
* Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI.
* Забезпечення антивірусного захисту в режимі реального часу.
* Використання евристичних технологій власної розробки під час сканування.
* Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку.
* Модуль захисту документів, що дає можливість перевіряти макроси Microsoft Office на наявність зловмисного коду.
* Можливість сканування файлів під час запуску ОС.
* Наявність вбудованого інструмента, що об'єднує в собі декілька утиліт для очищення залишків складних стійких загроз, таких як Conficker, Sirefef, Necurs та ін.
* Сканування комп'ютера у неактивному стані.
* Можливість визначення детальних параметрів роботи антивірусного сканера, таких як: визначення об’єктів та методів сканування, можливість встановлення максимального розміру та часу сканування файлу, максимальну глибину вкладення архіву та створення виключень.
* Захист від експлойтів який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків.
* Модуль, який глибоко аналізує запущені процеси та їх діяльність в файловій системі, що забезпечує додатковий рівень захисту від програм-вимагачів (Ransomeware).
* Розширений сканер пам'яті який відстежує підозрілі процеси та сканує їх, як тільки вони виникають, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами.
* Наявність системи виявлення вторгнень (HIPS), яка захищає комп’ютер від шкідливих програм і небажаної активності. Також цей модуль містить в собі майстер для створення правил та редактор правил для контролю запущених процесів, використовуваних файлів та розділів реєстру.
* Додаткова перевірка запущених процесів у хмарному репутаційному сервісі.
* Автоматична антивірусна перевірка змінних носіїв.
* Наявність інструменту, який зможе здійснювати контроль підключення до робочої станції змінних носіїв шляхом створення правил доступу, а саме: блокування, дозвіл, тільки читання, читання та запис, попередження.
* Можливість здійснювати контроль підключення до робочої станції зовнішніх пристроїв за типом пристрою, за виробником, моделлю або серійним номером пристрою.
* Можливість створювати групи дозволених або заборонених зовнішніх пристроїв.
* Можливість забороняти або дозволяти підключення зовнішніх пристроїв як для всіх, так і для окремих користувачів або груп Windows або домену.
* Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила контролю пристроїв.
* Забезпечення додаткового рівня захисту поштового трафіку на робочій станції шляхом інтеграції до поштового клієнту, з можливістю перевірки POP3, POP3S, SMTP, IMAP та IMAPS та перевірки поштових вкладень, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
* Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті.
* Наявність модуля захисту від спаму власної розробки з можливістю інтеграції до поштового клієнту, що забезпечує додатковий рівень захисту від спаму, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
* Можливість використовувати білі та чорні списки спам-адресатів як користувальницькі (гнучка персоналізація інтелектуального спам-модулю), так і глобальні, інформація до яких надходить з серверів оновлення.
* Забезпечення додаткового рівня захисту інтернет-трафіку шляхом перевірки HTTP, HTTPS трафіку, що дає можливість блокувати адреси таких небезпечних ресурсів, як фішингові сайти, сервери ботнетів, командні (C&C) сервери APT, а також сервери, що розповсюджують загрози класу «ransomware»,
* Можливість створення списків заблокованих, дозволених або виключених з перевірки URL-адрес.
* Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
* Можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах.
* Перевірка дійсності та цілісності сертифікатів SSL-трафіку, та можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим .
* Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).
* Наявність персонального брандмауера для здійснення мережевої фільтрації та захисту як від зовнішніх, так і локальних мережевих атак.
* Наявність у персональному брандмауеру інтерактивного режиму, що надає детальну інформацію про нове невідоме мережеве з'єднання та дає можливість не тільки створювати на ПК нове правило мережевої фільтрації для виявленого з'єднання, а й вказувати детальні налаштування для нього.
* Наявність у персональному брандмауеру режиму навчання, що дає можливість адміністратору віддалено налаштовувати дозвільні правила для мережевих додатків та обладнання.
* Наявність редактора правил, що дає можливість не тільки редагувати створені правила, а й керувати вбудованими правилами, яких достатньо для первинного ретельного захисту від несанкціонованих мережевих з'єднань та мережевих атак.
* Можливість створювати правила мережевої фільтрації для конкретних програм і сервісів.
* Можливість створювати для персонального брандмауеру різні профілі , які можуть автоматично переключатися, в залежності від того, до якої мережі підключено комп'ютер.
* Можливість використовувати у персональному брандмауері додаткову автентифікацію мережі з метою запобігання несанкціонованого підключення ПК до невідомих небезпечних мереж.
* Наявність додаткового функціоналу персонального брандмауеру, що дозволяє переглядати всю детальну інформацію по всіх наявних мережевих з'єднаннях, а також попереджати користувача про підключення до незахищеної мережі Wi-Fi.
* Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп’ютер.
* Можливість використання технології, яка забезпечує захист від загроз типу "ботнет"
* Захист уразливостей мережевого протоколу, що покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC, RDP і т.д.
* Наявність упроваджених методів виявлення різноманітних атак, що намагаються використовувати вразливості програмного забезпечення та надання докладнішої інформації про ідентифікатори CVE.
* Можливість переглядати на ПК автоматично заблоковані мережеві з'єднання та, за необхідністю, тимчасово дозволяти конкретні безпечні мережеві з'єднання.
* Наявність додаткового функціоналу персонального брандмауеру, що дає можливість переглядати на ПК перелік заблокованих IP-адрес, надає інформацію про причини потрапляння до чорного списку, та дозволяє зробити виключення для конкретних безпечних адрес.
* Наявність додаткового функціоналу персонального брандмауеру, який здатен виявляти ті зміни в мережевих програмах, що спричинили нові несанкціоновані мережеві з'єднання.
	+ Наявність модуля веб-контролю, що дає можливість обмежувати доступ до певних категорій сайтів.
	+ Можливість створювати правила фільтрації інтернет-трафіку для різних користувачів та груп ОС Windows або домену.
	+ Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила веб-фільтрації.
	+ Регламентне оновлення вірусних баз не менше 24 разів за добу.
	+ Отримання оновлення клієнтів з локального сховища на сервері, що дозволяє підтримувати актуальність антивірусного захисту в закритих ізольованих мережах, що не мають доступу до мережі Інтернет.
	+ Можливість створення дзеркала оновлень засобами антивірусної ПП.
	+ Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне.
	+ Можливість для портативних комп'ютерів отримувати оновлення з серверів виробника он-лайн, у разі перебування поза корпоративною мережею.
	+ Відкат оновлень з можливість повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.
	+ Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень.
	+ Наявність механізму контролю за станом безпеки та актуальністю оновлень ОС.
	+ Наявність інструменту для діагностики системи, який має можливість створювати знімки стану операційної системи для подальшого глибоко аналізу різноманітних аспектів роботи операційної системи, включаючи запущені процеси, контент реєстру, інстальоване ПЗ, мережеві з'єднання.
	+ Можливість визначення рівня критичності (небезпечний, невідомий, маловідомий, безпечний) значень різноманітних параметрів операційної системи, з метою виявлення несанкціонованих та небезпечних змін у операційній системі.
	+ Можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись в системі за визначений час.
	+ Можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання.
	+ Локальне зберігання журналів на робочих станціях.
	+ Наявність планувальника завдань, який дасть можливість створювати заплановані завдання, серед яких: запуск зовнішньої програми, перевірка файлів під час запуску системи, створення знімка стану системи, перевірка комп’ютера, оновлення вірусних баз та модулів програми.
	+ Можливість планування завдань, які запускатимуться одноразово, періодично, а також за умови виникнення конкретних подій.
	+ Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.
	+ Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.
	+ Можливість захисту від зміни параметрів антивірусного ПЗ паролем.
	+ Наявність режиму перевизначення політики, що дає системному адміністратору тимчасову можливість змінювати на ПК ті налаштування антивірусного ПЗ, що призначаються політикою, та недосяжні для редагування, з метою гнучкого налаштування антивірусного ПЗ у специфічному середовищі.
	+ Використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування.
	+ Можливість використання технологій машинного навчання для більш поглибленого аналізу коду з метою виявлення зловмисної поведінки та характеристик зловмисного програмного забезпечення.
	+ Графічний інтерфейс, сумісний із сенсорним екраном високої роздільної здатності.
	+ Можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача.
	+ Низьке споживання ресурсів ПК актуальними антивірусними продуктами (сукупно усіма процесами: графічний інтерфейс, процес комплексного захисту, служба віддаленого адміністрування): 50-100 МБ оперативної пам'яті, 2-35 % центрального процесору.
	+ Наявність багатомовного інсталятора, який містить в собі в тому числі українську мову.
	+ Наявність інструменту віддаленого управління.
* Автоматичне визначення ролей сервера для створювання автоматичних виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної операційної системи.
* Можливість крім основного вказати резервні сервери адміністрування.
* Наявність планувальника завдань, який дасть можливість створювати заплановані завдання, серед яких: запуск зовнішньої програми, перевірка файлів під час запуску системи, створення знімка стану системи, перевірка комп’ютера, оновлення вірусних баз та модулів програми. Можливість планування завдань, які запускатимуться одноразово, періодично та за умови виникнення конкретних подій.
* Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.
* Можливість роботи в кластерах як домена так і робочої групи.
* Можливість налаштовувати швидкодію, вказуючи кількість потоків сканування.
* Можливість налаштовувати режим запуску шляхом відключення графічного інтерфейсу для термінальних користувачів, що дає можливість зменшити навантаження на сервер, який працює у режимі серверу терміналів.
* Можливість встановлення агенту управління на ARM64 процесорах.
* Наявність функціоналу створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензії окремим філіям.
* Наявність функціоналу визначення адміністратора площадки або філії з відповідною частиною ліцензії.
* **Вимоги до інструменту віддаленого управління**
* Можливість централізованого управління антивірусним захистом всієї мережевої інфраструктури.
* Можливість будування ієрархічної структури адміністрування, що складається з головного серверу та підпорядкованих серверів, що дає можливість здійснювати централізоване управління антивірусним захистом робочих станцій, серверів, та мобільних пристроїв, що належать як головному, так і регіональним підрозділам.
* Інвентаризація обладнання, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.
* Інвентаризація ПЗ, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.
* Віддалена інсталяція антивірусного ПЗ для ОС Windows, Linux та Mac на кілька кінцевих точок одночасно засобами сервера адміністрування.
* Віддалена інсталяція користувальницького ПЗ одночасно засобами сервера адміністрування.
* Віддалена видалення встановленого користувальницького ПЗ засобами сервера адміністрування.
* Віддалене видалення антивірусного ПЗ для ОС Windows, Linux та Mac засобами сервера адміністрування.
* Можливість виконувати за допомогою інструменту віддаленого управління додаткові мережеві дії, такі як: завершення роботи та перезавантаження, відправка сигналу пробудження комп'ютера, відправка повідомлень, виконання конкретних інструкцій командного рядка на клієнтському комп'ютері, старт оновлення ОС клієнтського комп'ютера.
* Наявність інструменту для створення та редагування інсталяційних пакетів ОС Windows, Linux та Mac з попередньо встановленими настройками конфігурації, що дає можливість експортувати інсталяційні пакети для розгортання повноцінного антивірусного захисту на кінцевих точках в ізольованій мережі, а також на кінцевих точках, що потребують захисту, але тимчасово не мають з'єднання з сервером адміністрування.
* Наявність диспетчера користувачів, який дозволяє створювати різних користувачів сервера адміністрування, та призначати їм різні права доступу до окремих розділів, груп комп'ютерів на сервері адміністрування, що дає можливість надати різні права доступу для регіональних системних адміністраторів розгалуженої системи антивірусного захисту.
* Можливість аутентифікувати адміністраторів сервера адміністрування за допомогою груп безпеки AD.
* Можливість використовувати двофакторну аутентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованому підключенню до серверу централізованого управління.
* Наявність журналу аудиту, у якому реєструються і відстежуються всі зміни в конфігурації та всі дії, які виконують користувачі сервера адміністрування.
* Можливість віддалено активувати та деактивувати модулі захисту, такі як персональний брандмауер, захист в режимі реального часу, захист поштового клієнта, захист доступу до Інтернету, контроль пристроїв, веб-контроль, антиспам на окремо взятому клієнті.
* Можливість створювати та редагувати статичні групи та можливість імпорту з AD дерева комп'ютерів.
* Можливість налаштування автоматичного розподілу клієнтів по динамічних групах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань.
* Можливість імпорту користувачів та груп з AD, для подальшого використання їх для персоналізації правил контролю пристроїв та веб-контролю.
* Можливість використовувати як вбудовані так і користувальницькі політики, призначені для постійного обслуговування конфігураційних налаштувань антивірусних продуктів.
* Можливість здійснювати експорт/імпорт політик.
* Наявність панелі моніторингу, яка надає всю необхідну детальну інформацію стосовно рівня захисту безпеки інфраструктури, стану захищених кінцевих точок, а також стану самого сервера адміністрування.
* Наявність напередвстановлених шаблонів звітів, що можуть використовуватися як для панелі моніторингу, так і для формування різноманітних звітів.
* Можливість створювати та редагувати шаблони звітів, які використовуються як для панелі моніторингу, так і для формування звітів у форматах PDF, PS, CSV та подальшого зберігання за вказаним шляхом або відправлення на вказану електронну пошту.
* Підтримка інструментом віддаленого адміністрування наступних баз даних: MS SQL Server, MySQL.
* Можливість експортувати журнали в syslog для подальшої інтеграції з SIEM.
* Можливість створювати дзеркало оновлень за допомогою антивірусного продукту, спеціальної утиліти або проксі серверу.
* Можливість створення дзеркала оновлень на базі сторонніх HTTP-серверів.
* Веб-орієнтований інтерфейс, який дає можливість керувати сервером через будь-який браузер шляхом з'єднання, захищеного сертифікатом.
* Використання незалежного агенту, який дає можливість здійснювати як віддалене, так і автономне управління антивірусним продуктом на кінцевих точках, а також контролювати рівень захисту антивірусного захисту на робочих станціях, та стан операційної системи.
* Додатковий компонент, що дозволяє керувати антивірусним захистом на мобільних пристроях.
* Спеціальний компонент, який здійснює виявлення в мережі незахищених робочих станцій для подальшого розгортання антивірусного захисту.
* Захист з'єднань між компонентами сервера за допомогою як самостійно випущених сертифікатів, так й існуючих наявних сертифікатів.
* Інструмент для керування станом ліцензій (навіть без використання сервера адміністрування).
* Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станція до яких немає фізичного або віддаленого доступу.
* Можливість встановлення серверу адміністрування на ОС Windows та Linux.
* Постачання сервера адміністрування у розгорнутому вигляді, готовому для використання у таких віртуальних середовищах, як Microsoft Hyper-V, Oracle VirtualBox, VMware (ESXi/vSphere/Player/Workstation).
* Можливість використання антивірусних продуктів за умови, що управління ними буде здійснюватися існуючими наявними серверами адміністрування, які налаштовано на централізований моніторинг та управління всіма розгалуженими системами антивірусного захисту інфраструктури. На підтвердження відповідності пропозиції Учасника цій характеристиці на вимогу замовника учасник надає тестовий ключ тривалістю не менше 5 днів для його додавання до існуючого сервера керування.
* **Вимоги до захисту поштового серверу**
* Microsoft Exchange Server 2019, 2016, 2013, 2010, 2007.
* Перевірка вхідного та вихідного поштового трафіку на рівні транспортного протоколу.
* Захист бази даних поштових скриньок.
* Сканування листів в базі даних під час відкриття листа користувачем, в фоновому режимі.
* Сканування бази даних поштових скриньок за розкладом.
* Можливість виявлення реального типу файлу, що дозволяє застосовувати політики для певного типу вмісту електронних листів.
* Захист від спаму що оснований на використанні комплексу технологій: "чорні" списки реального часу, "чорні" списки серверів на основі DNS, використання цифрових відбитків, перевірка репутації, аналіз вмісту листа, фільтр Байеса, користувальницькі правила, користувальницькі "чорні" та "білі" списки.
* Робота з "сірими" списками що основана на специфікації RFC 821.
* Управління карантином пошти, можливість видаляти або відновлювати листи, що потрапили в карантин після сканування.
* Веб-інтерфейс для управління карантином пошти.
* Менеджер користувальницьких правил що дозволяє створювати умови фільтрації електронної пошти та дії що необхідно виконати з відфільтрованими повідомленнями.
* Можливість роботи в кластерах як домена так і робочої групи.
* Комплексний захист сервера, включаючи резидентний захист і сканування на вимогу.
* Наявність планувальника завдань.
* Можливість створення на сервері у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.
* Наявність eShell рядка, що дозволяє запускати скрипти для виконання дій, а також створювати/змінювати налаштування.
* Автоматичне створення виключень для критично важливих файлів операційної системи, що забезпечує мінімальний вплив на продуктивність роботи серверу.
* Можливість віддалено розгорнути, управляти та оновлювати антивірусні продукти для забезпечення безпеки в мережі.
* Можливість крім основного вказати резервний сервер адміністрування.
* Застосування політик, моніторинг виявлень і налаштування програми мають здійснюватися з єдиної консолі.
* Наявність веб-панелі, що забезпечує повний контроль над корпоративною мережею в режимі реального часу.
* Можливість створювати докладні та повні журнали і статистику про стан безпеки.
* Наявність журналу спаму з відображенням відправника, одержувача, оцінку спаму, причину класифікації, а також виконані дії.
* Наявність журналу «сірих» списків — відображає «сірого» відправника, одержувача, виконані дії та статус.
* Моніторинг продуктивності сервера в режимі реального часу.
* Можливість відправляти підозрілі вкладення листів з поштового серверу на аналіз до хмари
* Використання технологій машинного навчання під час первинного аналізу відправлених файлів.
* Можливість здійснювати безперервне спостерігання за активністю відправлених файлів (30 днів за замовчуванням), що дозволяє виявляти навіть ті загрози, що здатні обходити класичну пісочницю.
* Можливість здійснювати автоматичне блокування файлів, що спричинили зловмисну активність під час первинного аналізу або підчас тривалого спостерігання у хмарі.
* Можливість забезпечити швидку реакцію, за результатами первинного аналізу, шляхом блокування 0-денних загроз (від декілька секунд до 10 хвилин).
* Можливість здійснювати гнучкі налаштування відправки підозрілих файлів та визначення реакції після первинного аналізу або виявлення зловмисної активності під час тривалого спостереження у хмарі.

Запропоновані рішення повинні мати діючий експертний висновок ДССЗЗІ.

* **Вимоги до двуфакторної аутентифікації**

1. Можливість додання 2FA для безпечного доступу входу в як локальний обліковий запис, так і доменний обліковий запис системи під управлінням: Miscrosoft Windows, Linux або MAC OS X.

2. Можливість отримання паролів 2FA за допомогою смс-повідомлень, push-повідомлень, OTP.

3. Підтримку апаратних токенів, які працюють по стандартам OATH, HOTP, TOTP,FIDO,FIDO2.

4. Можливість додання 2FA для веб-додатків Microsoft: Microsoft Outlook Web App, Microsoft Exchange, Microsoft SharePoint, Microsoft Exchange Mailbox Server Role, Microsoft SharePoint Foundation, Microsoft Dynamics CRM, Microsoft Remote Desktop Web Access, Microsoft Remote Desktop Gateway, Microsoft Terminal Services Web Access, Microsoft Exchange Admin Center.

5. Наявність API, яка дозволяє швидко додавати двофакторну аутентифікацію в наявні додатки.

6. Наявність пакету SDK, що надає доступ до функцій керування користувачами та їх аутентифікаціями.

7. Захист VPN ТА VDI систем, таких як : Microsoft Forefront Threat Management Gateway, Barracuda, F5 FirePass, Cisco ASA IPSEC,Cisco ASA SSL, Fortinet FortiGate, Citrix Access Gateway, Juniper, Citrix NetScaler, Palo Alto, Check Point Software, SonicWall,Netasq, VMware Horizon View и Citrix XenApp, Cyberoam.

8. Можливість захисту RADIUS PAM для Linux, Mac.

9. Наявність Identity Provider Connector для забезпечення 2FA хмарних служб (постачальником послуг) і постачальником ідентифікаційних даних, таких як: OpenAM, Okta, Azure AD, AD FS, Shibboleth, Keycloak, Dropbox, Confluence.

10. Захист через SSO та Microsoft Active Directory Federation Services для входу до Office 365 або Azure.

11. Інформування користувача про спробу авторизації з можливістю підтвердити або відхилити подальшу автентифікацію.

12. Наявність системи звітності, що можуть використовуватися як для панелі моніторингу, так і для формування звітів.

13. Наявність журналу аудиту, у якому реєструються і відстежуються всі зміни в конфігурації, запуск та зупинки служби двофакторної аутентифікації.

14. Можливість інтеграції з SIEM та іншими системами моніторингу, аналітики та реагування

15. Можливість для адміністратора надавати альтернативний одноразовий пароль OTP у разі, якщо коли користувач немає доступу до токену або до мобільного додатку.

16. Можливість імпортувати користувачів у спеціальні області за допомогою файлу CSV або LDF

17. Можливість використання 2FA для безпечного режиму, блокуванні облікового запису Windows, використання UAC.

18. Можливість налаштувати використання 2FA для користувачів, які не мають підключення до серверу 2FA.

19. Можливість обмежити кількість використання одноразовий паролів для комп'ютерів, які не мають підключення до серверу 2FA.

20. Наявність захисту від підбору одноразового паролю шляхом блокування користувача.

21. Наявність системи сповіщень про вибрані типи дій.

22. Можливість виключення з 2FA для списку IP-адрес.

23. Можливість налаштування користувацького способу доставлення паролів OTP.

24. Можливість синхронізації користувачів за допомогою LDAP та Mac Open Directory.

25. Наявність експертного рішення ДССЗЗІ на продукту.

**Додатково:**

1. Учасник повинен у складі своєї Пропозиції надати копію документа, що підтверджує статус Учасника як офіційного представника (партнера) виробника в Україні. На підтвердження надати копію авторизаційного листа від виробника або його офіційного представництва в Україні для даної закупівлі;

 **Технічні, якісні характеристики предмета закупівлі, повинні передбачати необхідність застосування заходів із захисту довкілля,** відповідати вимогам Законів України «Про охорону навколишнього природного середовища», «Про забезпечення санітарного та епідеміологічного благополуччя населення» та інших чинних нормативно-правових актів України з питань екологічної безпеки, охорони навколишнього природного середовища, пожежної та техногенної безпеки, охорони праці та виробничої санітарії.