|  |
| --- |
| Назва закупівлі: **Ліцензії на використання програмного забезпечення ESET PROTECT Complete з локальним управлінням 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 з особливостями**  Очікувана вартість: **506 000,00 грн з ПДВ**  Дата оприлюднення: **09 червня 2023 року**  Детальна інформація за посиланням: <https://prozorro.gov.ua/tender/UA-2023-06-09-007963-a> |
| **ІНФОРМАЦІЯ ПРО НЕОБХІДНІ ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ**  на закупівлю: | |

**надання Ліцензії на використання програмної продукції ESET PROTECT Complete з локальним управлінням та ESET Secure Authentication**

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

|  |  |  |
| --- | --- | --- |
| № з/п | Найменування Ліцензії \* | Кількість  шт. |
|  | Програмна продукція (ліцензія) 'ESET PROTECT Complete з локальним управлінням' (G). На 1 рік. Поновлення. Для захисту 550 об'єктів. | 1 |
|  | Програмна продукція (ліцензія) '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**

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

- обслуговування 24х7х365 - 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;

* **Вимоги до рішення для захисту робочих станцій під управління несерверних ОС**

1. Надання захисту від: вірусів, троянського ПЗ, рекламного ПЗ, фішингу, а також шпигунського ПЗ.
2. 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.
3. 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 налаштування системи, а також виконувати неочікувані дії або дії, не підтверджені користувачем.
4. Надання захисту від потенційно небезпечних програм - різноманітного ПЗ, що може використовуватися для зловмисних цілей, таких як несанкціонований віддалений доступ, викрадення або злам паролів, клавіатурні шпигуни тощо.
5. Надання захисту від підозрілих програм – програм, які стиснуті тими пакувальниками або протекторами, що часто використовують зловмисники за для того, щоб запобігти виявленню шкідливого програмного забезпечення.
6. Надання захисту від небезпечних програм руткітів, які надають зловмисникам з Інтернету необмежений доступ до системи, водночас приховуючи свою присутність в операційній системі.
7. Можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування.
8. Можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення в роботі або впливати на продуктивність системи.
9. Можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання в процес роботи ОС.
10. Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI.
11. Забезпечення антивірусного захисту в режимі реального часу.
12. Використання евристичних технологій власної розробки під час сканування.
13. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку.
14. Модуль захисту документів, що дає можливість перевіряти макроси Microsoft Office на наявність зловмисного коду.
15. Можливість сканування файлів під час запуску ОС.
16. Наявність вбудованого інструмента, що об'єднує в собі декілька утиліт для очищення залишків складних стійких загроз, таких як Conficker, Sirefef, Necurs та ін.
17. Сканування комп'ютера у неактивному стані.
18. 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.
19. Використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування
20. Можливість використання технологій машинного навчання для більш поглибленого аналізу коду з метою виявлення зловмисної поведінки та характеристик зловмисного програмного забезпечення.
21. Модуль захисту від експлойтів який забезпечує захист від загроз здатних використовувати уразливості різноманітних додатків, таких як Java, Flash тощо.
22. Модуль, який глибоко аналізує запущені процеси та їх діяльність в файловій системі, що забезпечує додатковий рівень захисту від програм-вимагачів (Ransomware).
23. Модуль сканування оперативної пам'яті, який здатен відстежувати роботу підозрілих запущених процесів, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами.
24. Наявність системи виявлення вторгнень (HIPS), що слідкує за запуском програм та змінами в системному реєстрі та захищає комп’ютер від шкідливих програм і небажаної активності.
25. Можливість створювати власні правила для контролю запущених процесів, виконуваних файлів та розділів реєстру.
26. Додаткова перевірка запущених процесів у хмарному репутаційному сервісі.
27. Автоматична антивірусна перевірка змінних носіїв.
28. 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.
29. Можливість здійснювати контроль підключення до робочої станції зовнішніх пристроїв за типом пристрою, за виробником, моделлю або серійним номером пристрою.
30. Можливість створювати групи дозволених або заборонених зовнішніх пристроїв.
31. Можливість забороняти або дозволяти підключення зовнішніх пристроїв як для всіх, так і для окремих користувачів або груп Windows або домену.
32. Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила контролю пристроїв.
33. 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.
34. Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті.
35. Забезпечення додаткового рівня захисту інтернет-трафіку шляхом перевірки HTTP, HTTPS трафіку, що дає можливість не тільки блокувати файли, що передаються цими протоколами, а й блокувати адреси таких небезпечних ресурсів, як фішингові сайти, сервери ботнетів, командні (C&C) сервери APT, а також сервери, що розповсюджують загрози класу «ransomware».
36. Можливість створення списків заблокованих, дозволених або виключених з перевірки URL-адрес.
37. Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.
38. Можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах.
39. Перевірка дійсності та цілісності сертифікатів SSL-трафіку.
40. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим.
41. Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).
42. Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп’ютер.
43. Можливість використання технології, яка забезпечує захист від загроз типу "ботнет"
44. Захист уразливостей мережевого протоколу, що покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC, RDP і т.д.
45. Наявність упроваджених методів виявлення різноманітних атак, що намагаються використовувати вразливості програмного забезпечення та надання докладнішої інформації про ідентифікатори CVE
46. Регламентне оновлення вірусних баз не менше 24 разів за добу.
47. 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.
48. Можливість створення дзеркала оновлень на базі рішень для захисту кінцевих точок.
49. Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне.
50. Можливість для портативних комп'ютерів отримувати оновлення з серверів виробника он-лайн, у разі перебування поза корпоративною мережею.
51. Відкат оновлень з можливістю повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.
52. Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень.
53. Наявність механізму контролю за станом безпеки та актуальністю оновлень ОС.
54. 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.
55. Можливість визначення рівня критичності (небезпечний, невідомий, маловідомий, безпечний) значень різноманітних параметрів операційної системи, з метою виявлення несанкціонованих та небезпечних змін у операційній системі.
56. Можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись в системі за визначений час.
57. Можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання.
58. Локальне зберігання журналів на робочих станціях.
59. 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.
60. Можливість планування завдань, які запускатимуться одноразово, періодично, а також за умови виникнення конкретних подій.
61. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.
62. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.
63. Можливість захисту паролем параметрів рішення для захисту кінцевої точки.
64. 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.
65. Графічний інтерфейс, сумісний із сенсорним екраном високої роздільної здатності.
66. Можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача.
67. Можливість віддаленого встановлення на клієнтську робочу станцію
68. Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ.
69. Сумісність з існуючим сервером централізованого керування та активація антивірусного ПЗ шляхом додавання ключа до існуючого сервера керування. Для підтвердження відповідності пропозиції Учасника цій характеристиці та можливості перевірки відповідності запропонованого рішення заявленим технічним вимогам, на вимогу Замовника, Учасник надає тестовий ключ тривалістю не менше 5 днів для його додавання до існуючого сервера керування.
70. Можливість крім основного вказати резервні сервери адміністрування.
71. Наявність багатомовного інсталятора, який містить в собі в тому числі українську мову.
72. Microsoft Windows 7 (Professional або вище); Microsoft Windows 8 (Professional або вище); Microsoft Windows 8.1 (Professional або вище); Microsoft Windows 10; Microsoft Windows 11; Підтримка Microsoft Windows 10 Multi-session та Azure virtualized Windows 10; Ubuntu Desktop 18.04 LTS 64-bit, Ubuntu Desktop 20.04 LTS, Red Hat Enterprise Linux 7 та 8, SUSE Linux Enterprise Desktop 15.
73. Учасник повинен надати Замовнику копії діючих Експертних висновків (на рішення або на його складові, які будуть використовуватися Замовником, згідно технічних вимог, викладених вище), зареєстрованих в Адміністрації Державної служби спеціального зв’язку та захисту інформації України щодо відповідності вимогам нормативних документів системи технічного захисту інформації в Україні.

* **Вимоги до рішення для захисту робочих станцій під управління серверних ОС**

1. Підтримка ОС: Microsoft Win. Server 2012R2, 2012, 2008R2, 2008, Microsoft Win. Server Core 2012R2, 2012, 2008R2, 2008 Core; RedHat Enterprise Linux (RHEL) 7, RedHat Enterprise Linux (RHEL) 8, RedHat Enterprise Linux (RHEL) 9, CentOS 7, Ubuntu Server 18.04 LTS, Ubuntu Server 20.04 LTS, Ubuntu Server 22.04 LTS, Debian 10, Debian 11, SUSE Linux Enterprise Server (SLES) 12,SUSE Linux Enterprise Server (SLES) 15,Oracle Linux 8, Amazon Linux 2.
2. Автоматичне визначення ролей сервера для створювання автоматичних виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної операційної системи.
3. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку.
4. Сканування Hyper-V на наявність вірусів, що дозволяє сканувати диски сервера Microsoft Hyper-V Server, тобто віртуальних машин (ВМ), без необхідності установки будь-яких агентів на відповідних віртуальних машинах.
5. Модуль захисту документів Microsoft Office, що дає можливість перевіряти макроси на наявність зловмисного коду.
6. Додатковий рівень захисту користувачів від програм-вимагачів контролює та оцінює всі програми на основі їхньої поведінки та репутації.
7. Можливість сканування файлів під час запуску ОС.
8. 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.
9. Сканування комп'ютера у неактивному стані.
10. 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.
11. Автоматична антивірусна перевірка змінних носіїв.
12. Контроль змінних носіїв з можливістю створення правил за типом пристрою, діями, виробником, моделлю та серійним номером пристрою.
13. Наявність інструменту, який зможе здійснювати контроль підключення до робочої станції периферійних пристроїв шляхом створення правил доступу за типом пристрою, за рівнем доступу, за виробником, моделлю або серійним номером пристрою. Правила можуть створюватись як для всіх, так і для окремих користувачів або груп Windows.
14. 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.
15. Забезпечення захисту поштового клієнту на робочій станції з можливістю інтеграції до поштового клієнту, перевіркою POP3, POP3S, SMTP, IMAP та IMAPS та забезпечення перевірки поштових вкладень.
16. Перевірка HTTP, HTTPS трафіку з можливістю створення листів виключених з перевірки, заблокованих та дозволених URL-адрес.
17. Можливість перевірки протоколу SSL та перевірки дійсності та цілісності сертифікатів. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим.
18. Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).
19. Регламентне оновлення вірусних баз не менше 24 разів за добу.
20. Можливість крім основного вказати резервні сервери адміністрування.
21. Наявність механізму контролю за актуальністю оновлень ОС.
22. 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. Завдяки вмінню порівнювати різні знімки стану системи цей інструмент може виявити зміни, які відбулись в системі. Також він може створювати та виконувати скрипти, що дасть можливість зупиняти запущені процеси, видаляти гілки реєстру, блокувати мережеві з'єднання.
23. 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.
24. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.
25. Можливість роботи в кластерах як домена так і робочої групи.
26. Можливість налаштовувати швидкодію, вказуючи кількість потоків сканування.
27. Можливість налаштовувати режим запуску шляхом відключення графічного інтерфейсу для термінальних користувачів, що дає можливість зменшити навантаження на сервер, який працює у режимі серверу терміналів.
28. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.
29. Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ.
30. Можливість захисту від зміни параметрів антивірусного ПЗ паролем.
31. Наявність спеціальної технології, яка значно знижує навантаження на віртуальні робочі станції, а також на гіпервізор у цілому.

* **Вимоги до захисту поштового серверу**

1. Підтримка ОС: Microsoft Exchange Server 2022, 2019 2016, 2013, 2010, 2007.
2. Перевірка вхідного та вихідного поштового трафіку на рівні транспортного протоколу.
3. Захист бази даних поштових скриньок.
4. Сканування листів в базі даних під час відкриття листа користувачем, в фоновому режимі.
5. Сканування бази даних поштових скриньок за розкладом.
6. Можливість виявлення реального типу файлу, що дозволяє застосовувати політики для певного типу вмісту електронних листів.
7. Захист від загроз що знаходяться у поштових вкладеннях з детальним налаштуванням параметрів та використання технології ThreathSense
8. Можливість використовувати додаткові технології, що дозволяють перевірити, чи не підроблений домен відправника (SPF), та визначити відправника повідомлення за цифровим підписом (DKIM)
9. Можливість фільтрації контенту, що дозволяє фільтрувати поштовий трафік на основі наступних параметрів: тема, заголовок, назва вкладення, тип вкладення, розмір повідомлення, текст повідомлення, наявність захищеного архіву, результати перевірки DKIM, SPF, DMARC та інші.
10. Захист від спаму, що оснований на використанні комплексу технологій: «чорні» списки серверів на основі DNS (DNSBL) та серверів реального часу (RBL), використання цифрових відбитків, перевірка репутації, аналіз вмісту листа, користувальницькі правила, користувальницькі «чорні» та «білі» списки. Робота з "сірими" списками що основана на специфікації RFC 821.
11. Розширені налаштування механізму антиспаму на базі графічного інтерфейсу користувача.
12. Встановлення лише необхідних компонентів на основі вибору користувача
13. Наявність модуля, який забезпечує захист поштового сервера від експлойтів, загроз здатних використовувати уразливості Java, Flash та інших додатків.
14. Наявність модуля, який відстежує підозрілі процеси в оперативній пам'яті поштового сервера та сканує їх, як тільки вони виникають, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами.
15. Наявність системи виявлення вторгнень (HIPS), яка захищає поштовий сервер 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.
16. Автоматичне визначення ролей сервера та додавання виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної операційної системи.
17. Надання захисту від: шкідливих програм, троянського ПЗ, клавіатурних шпіонів, рекламного ПЗ, фішингу, шпигунського ПЗ, руткітів, скриптів, потенційного небажаного та небезпечного ПЗ, мережевих атак та спаму.
18. Забезпечення захисту в режимі реального часу.
19. Використання евристичних технологій під час сканування.
20. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку.
21. Модуль захисту документів Microsoft Office, що дає можливість перевіряти макроси на наявність зловмисного коду.
22. Захист від експлойтів який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків
23. Можливість сканування файлів під час запуску операційної системи.
24. Розширенний сканер пам'яті який відстежує підозрілі процеси та сканує їх, як тільки вони виникають, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами.
25. Сканування комп'ютера у неактивному стані.
26. 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.
27. Автоматична антивірусна перевірка змінних носіїв.
28. Контроль змінних носіїв з можливістю створення правил за типом пристрою, діями, виробником, моделлю та серійним номером пристрою.
29. Наявність інструменту, який зможе здійснювати контроль підключення до робочої станції периферійних пристроїв шляхом створення правил доступу за типом пристрою, за рівнем доступу, за виробником, моделлю або серійним номером пристрою. Правила можуть створюватись як для всіх, так і для окремих користувачів або груп Windows.
30. 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.
31. Додаткова перевірка запущених процесів у хмарному репутаційному сервісі.
32. Забезпечення захисту поштового клієнту на робочій станції з можливістю інтеграції до поштового клієнту, перевіркою POP3, POP3S, SMTP, IMAP та IMAPS та забезпечення перевірки поштових вкладень.
33. Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті.
34. Перевірка HTTP, HTTPS трафіку з можливістю створення листів виключених з перевірки, заблокованих та дозволених URL-адрес.
35. Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням.
36. Можливість перевірки протоколу SSL та перевірки дійсності та цілісності сертифікатів. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим .
37. Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).
38. Регламентне оновлення вірусних баз не менше 24 разів за добу.
39. Отримання оновлення клієнтів з локального дзеркала на сервері.
40. Можливість створення дзеркала оновлень засобами антивірусного ПЗ.
41. Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне.
42. Відкат оновлень з можливість повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.
43. Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень.
44. Можливість крім основного вказати резервні сервери адміністрування.
45. 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. Завдяки вмінню порівнювати різні знімки стану системи цей інструмент може виявити зміни, які відбулись в системі. Також він може створювати та виконувати скрипти, що дасть можливість зупиняти запущені процеси, видаляти гілки реєстру, блокувати мережеві з'єднання.
46. Можливість налаштовувати швидкодію, вказуючи кількість потоків сканування.
47. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.
48. Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ.
49. Можливість захисту від зміни параметрів антивірусного ПЗ паролем.
50. Наявність спеціальної технології, яка значно знижує навантаження на віртуальні робочі станції, а також на гіпервізор у цілому.
51. Управління карантином пошти, можливість видаляти або відновлювати листи, що потрапили в карантин після сканування.
52. Веб-інтерфейс для управління карантином пошти.
53. Менеджер користувальницьких правил що дозволяє створювати умови фільтрації електронної пошти та дії що необхідно виконати з відфільтрованими повідомленнями.
54. Можливість роботи в кластерах як домена так і робочої групи.
55. Комплексний захист сервера, включаючи резидентний захист і сканування на вимогу.
56. Наявність планувальника завдань.
57. Можливість створення на сервері у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.
58. Наявність eShell рядка, що дозволяє запускати скрипти для виконання дій, а також створювати/змінювати налаштування.
59. Автоматичне створення виключень для критично важливих файлів операційної системи, що забезпечує мінімальний вплив на продуктивність роботи серверу.
60. Можливість віддалено розгорнути, управляти та оновлювати антивірусні продукти для забезпечення безпеки в мережі.
61. Можливість крім основного вказати резервний сервер адміністрування.
62. Застосування політик, моніторинг виявлень і налаштування програми мають здійснюватися з єдиної консолі.
63. Наявність веб-панелі, що забезпечує повний контроль над корпоративною мережею в режимі реального часу.
64. Можливість створювати докладні та повні журнали і статистику про стан безпеки.
65. Наявність журналу спаму з відображенням відправника, одержувача, оцінку спаму, причину класифікації, а також виконані дії.
66. Наявність журналу «сірих» списків — відображає «сірого» відправника, одержувача, виконані дії та статус.
67. Моніторинг продуктивності сервера в режимі реального часу.
68. Можливість відправляти підозрілі вкладення листів з поштового серверу на аналіз до хмари
69. Використання технологій машинного навчання під час первинного аналізу відправлених файлів
70. Можливість здійснювати автоматичне блокування файлів, що спричинили зловмисну активність під час первинного аналізу або підчас тривалого спостерігання у хмарі.
71. Можливість забезпечити швидку реакцію, за результатами первинного аналізу, шляхом блокування 0-денних загроз (від декілька секунд до 10 хвилин).
72. Наявність системи звітності, яка надає звіти про результат дослідження відправлених до хмари зразків.
73. Можливість здійснювати гнучкі налаштування відправки підозрілих файлів та визначення реакції після первинного аналізу або виявлення зловмисної активності під час тривалого спостереження у хмарі.
74. Сумісність з існуючим сервером централізованого керування та активація антивірусного ПЗ шляхом додавання ключа до існуючого сервера керування. Для підтвердження відповідності пропозиції Учасника цій характеристиці та можливості перевірки відповідності запропонованого рішення заявленим технічним вимогам, на вимогу Замовника, Учасник надає тестовий ключ тривалістю не менше 5 днів для його додавання до існуючого сервера керування.

* **Вимоги до інструменту віддаленого управління антивірусними рішеннями:**

1. Можливість централізованого управління антивірусним захистом всієї мережевої інфраструктури.
2. 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.
3. Інвентаризація обладнання, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.
4. Інвентаризація програмного забезпечення, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.
5. Віддалена інсталяція антивірусного програмного забезпечення для ОС Windows, Linux та Mac на кілька кінцевих точок одночасно.
6. Віддалена інсталяція користувальницького програмного забезпечення.
7. Можливість віддаленого видалення встановленого користувальницького ПЗ.
8. Віддалене видалення антивірусного програмного забезпечення для ОС Windows, Linux та Mac
9. 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 операційної системи клієнтського комп'ютера.
10. Наявність інструменту для створення та редагування інсталяційних пакетів для операційних систем 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.
11. 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.
12. Можливість аутентифікувати адміністраторів за допомогою груп безпеки AD.
13. Можливість використовувати двофакторну аутентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованному підключенню до серверу централізованого управління.
14. Наявність журналу аудиту, у якому реєструються і відстежуються всі зміни в конфігурації і всі дії, які виконують користувачі сервера адміністрування.
15. Можливість створювати та редагувати статичні групи та можливість імпорту з AD дерева комп'ютерів.
16. Можливість налаштування автоматичного розподілу клієнтів по динамічних групах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань.
17. Можливість імпорту користувачів та груп з AD, для подальшого використання їх для персоналізації правил контролю пристроїв та веб-контролю.
18. Можливість використовувати як вбудовані так і користувальницькі політики, призначені для постійного обслуговування конфігураційних налаштувань антивірусних продуктів. Можливість здійснювати експорт/імпорт політик.
19. Наявність панелі моніторингу, яка надає всю необхідну детальну інформацію стосовно рівня захисту безпеки інфраструктури, стану захищених кінцевих точок, а також стану самого сервера адміністрування.
20. Наявність близько 100 передвстановлених шаблонів звітів, що можуть використовуватися як для панелі моніторингу, так і для формування різноманітних звітів.
21. Можливість створювати та редагувати шаблони звітів, які використовуються як для панелі моніторингу, так і для формування звітів у форматах PDF, CSV та подальшого зберігання за вказаним шляхом або відправлення на вказану електронну пошту.
22. Підтримка інструментом віддаленого адміністрування наступних баз даних: MS SQL Server, MySQL.
23. Можливість експортувати журнали в syslog для подальшої інтеграції з SIEM.
24. Можливість налаштовувати параметри журналів та звітів або вибрати з більш ніж 50 шаблонів для різних систем/клієнтів.
25. Можливість створювати дзеркало оновлень за допомогою антивірусного продукту, спеціальної утиліти або проксі серверу.
26. Можливість створення дзеркала оновлень на базі сторонніх HTTP-серверів.
27. Веб-орієнтований інтерфейс, який дає можливість керувати сервером через будь який браузер шляхом з'єднання, захищеного сертифікатом.
28. Використання незалежного агенту, який дає можливість здійснювати віддалене управління антивірусним продуктом на кінцевих точках, а також контролювати рівень захисту антивірусного захисту на робочих станціях, та стан операційної системи.
29. Можливість відслідковувати все встановлене на робочій станції ПЗ, а також видаляти встановлене ПЗ за вибором.
30. Додатковий компонент, що дозволяє керувати антивірусним захистом на мобільних пристроях
31. Спеціальний компонент, який здійснює виявлення в мережі незахищених робочих станцій для подальшого розгортання антивірусного захисту.
32. Захист з'єднань між компонентами сервера за допомогою як самостійно випущених сертифікатів, так і існуючих наявних сертифікатів.
33. Інструмент для керування станом ліцензій (навіть без використання сервера адміністрування).
34. Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станція до яких немає фізичного або віддаленого доступу
35. Можливість встановлення серверу адміністрування на ОС Windows та Linux.
36. Постачання сервера адміністрування у розгорнутому вигляді, готовому для використання у таких віртуальних середовищах, як Microsoft Hyper-V, Oracle VirtualBox, VMware (ESXi/vSphere/Player/Workstation).
37. Підтримка систем віртуалізації таких як VMware Horizon 8.x або Citrix XenCenter/XenServer 8+.
38. Можливість обирати варіанти обробки ідентифікаторів клонованих комп’ютерів, такі як зіставляння з наявними комп’ютерами або створення нових комп’ютерів.
39. Можливість визначати параметри шаблону іменування VDI для миттєвих клонів або каталогів машин.
40. 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 регіональних та центрального підрозділів.
41. Наявність передвстановлених шаблонів в системі сповіщень для інформування про некоректну ідентифікацію клонованих машин, що дає можливість сповіщати про некоректно налаштовану інтеграцію с системами VDI.
42. Наявність автоматичного оновлення агенту управління, що дає можливість без втручання адміністраторів використовувати актуальні версії.
43. Наявність механізму розподілу автоматичного процесу оновлення, що дозволяє знизити навантаження на мережу та комп'ютери в цілому.
44. Наявність функціоналу створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензії окремим філіям.
45. Наявність функціоналу визначення адміністратора площадки або філії з відповідною частиною ліцензії.
46. Можливість встановлення агенту управління на ARM64 процесорах.

* **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 документ, що підтверджує статус Учасника як офіційного представника (партнера) виробника в Україні, а саме - авторизаційний лист від виробника (дилера, дистриб’ютора) щодо можливості постачання предмету даної закупівлі. Лист має бути адресований замовнику торгів та містити ідентифікатор закупівлі, назву предмету закупівлі, кількість, інформацію щодо термінів постачання/надання. Повноваження дилера/дистриб’ютора повинні бути підтверджені шляхом надання копії документу, який свідчить про передачу повноважень від виробника представляти його інтереси на території України.

**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.

**У разі, якщо пропозиція учасника не відповідає умовам технічної специфікації та іншим вимогам щодо предмета закупівлі встановленим даною тендерною документацією, або учасник не в змозі виконати умови які визначені Замовником в даній тендерній документації, пропозиція відхиляється.**