

Formularz asortymentowo-ilościowo-cenowy z zestawieniem oferowanych parametrów technicznych i użytkowych

Nazwa Wykonawcy

PAKIET NR 2

I.p.	Nazwa przedmiotu zamówienia	Ilość	Cena jednostkowa netto [PLN]	Wartość netto [PLN]	VAT %	VAT w zł	Wartość brutto [PLN]
I.	ESET – wznowienie, rozszerzenie i przejście na ESET PROTECT Enterprise (EDR)	1 kpl.	153,85	20 000,50	23	4 600,12	24 600,62
Razem				20 000,50	23	4 600,12	24 600,62

Lp.	Opis minimalnych wymagań Zamawiającego dotyczących warunków, parametrów technicznych, właściwości użytkowych i innych dla oferowanego przedmiotu zamówienia	Opis oferowanego przedmiotu zamówienia – należy wpisać oferowane parametry odnoszące się do wymagań dotyczących warunków, parametrów technicznych, właściwości użytkowych i innych dla oferowanego przedmiotu zamówienia określonych przez Zamawiającego - podaje Wykonawca
I.	ESET – wznowienie, rozszerzenie i przejście na ESET PROTECT Enterprise (EDR)	
	Nazwa	ESET PROTECT Enterprise ON-PREM
	Ilość licencji - stanowisk	130
	Producent /Firma /kraj pochodzenia	ESET, spol. s r.o. / Słowacja
	Ważność licencji	03.03.2025 r.
Wymagania		
1.	Zgodne z SIWZ	TAK

**UWAGA: brak potwierdzenia spełnienia przez Wykonawcę minimalnych parametrów i warunków dla urządzenia wymaganych przez Zamawiającego będzie traktowane jako brak danego parametru i będzie skutkowało odrzuceniem oferty.*

„Oświadczamy, że oferowane urządzenia spełniają wymagania techniczne, zawarte w powyższym i poniższym opisie, są kompletne, fabrycznie nowe i będą gotowe do użytku bez żadnych dodatkowych kosztów”

Lubin dnia 04.11.2022 r.

[podpis elektroniczny osoby uprawnionej]

Szczegółowy opis zamówienia

Pakiet nr 2

ESET – wznowienie, rozszerzenie i przejście na ESET PROTECT Enterprise (EDR)

**ESET Endpoint Security Suite kontynuacja - 110 stacji końcowych (klucz licencyjny)
Rozszerzenie do minimum 130 stacji końcowych i dodanie funkcjonalności EDR
Utrzymanie ważności licencji minimum do dnia 03.03.2025 roku.**

Dodatkowo w ramach dostarczenia oprogramowania szkolenie:

- Pełne wsparcie z instruktązem z przeprowadzenia migracji na stanowiskach oraz wsparcie z wdrożeniem na serwerze
- opowiedzenie o relacji działania ESET PROTECT – ESET INSPECT(EDR)
- omówienie różnic między EEA(Eset endpoint antywirus, a Eset endpoint security)
- zarządzanie administratorami i ich uprawnieniami
- polityki i dziedziczenie
- grupy statyczne i dynamiczne
- zapora osobista
- kontrola dostępu do stron internetowych
- dodawanie wykluczeń w Eset Inspect(EDR)
- analiza logów rozwiązywania Eset Inspect(EDR)
- przedstawienie obsługi reguł

Czas trwania szkoleń podzielony na 2 etapy nie powinien być krótszy sumarycznie niż 5 godzin.

zawierający: (Ochrona przed szkodliwym oprogramowaniem dla stacji roboczych, Ochrona przed szkodliwymi programami dla serwerów plików (możliwość instalacji dla min. 30% licencji), Ochrona i zarządzanie urządzeniami mobilnymi, Kontrola (aplikacji, urządzeń, sieci), Konsola zarządzająca) lub równoważny**

** za równoważny Zamawiający uzna oprogramowanie spełniające standardy jakościowe systemu wymagane przez Zamawiającego oraz współpracujące bez zakłóceń z systemami operacyjnymi stacji roboczych (Microsoft Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 10) i serwerów (Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016, 2019) posiadanymi przez Zamawiającego. W przypadku zaoferowania systemu równoważnego Zamawiający wymaga zainstalowania i skonfigurowania dostarczonego oprogramowania na wskazanych serwerach i stacjach roboczych zabezpieczanych dotychczas przez oprogramowanie ESET (w tym odinstalowania działającego na tych stacjach oprogramowania ESET). Skonfigurowania zaoferowanego oprogramowania (utworzenie odpowiednich grup komputerów, przypisanie komputerów do poszczególnych grup, zdefiniowania odpowiednich reguł aktualizacji, skanowania. Firewall dla poszczególnych grup komputerów i konsoli zarządzającej zgodnie z wymaganiami Zamawiającego). Przeszkolenia administratorów Zamawiającego 3 osoby z administracji, konfiguracji i instalacji wdrożonego oprogramowania (min. 2 dni po 3 godz. szkolenia). Instalacja i konfiguracja ma przebiegać w sposób nie zakłócający pracy użytkowników, stacji roboczych oraz serwerów.
Opis wymagań dostarczanego systemu:

1. Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 10, Windows 11
2. Wersja programu dla stacji roboczych Windows dostępna co najmniej w języku polskim.

Ochrona antywirusowa i antyspyware

3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
4. Wbudowana technologia do ochrony przed rootkitami.
5. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami
9. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
10. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
11. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
12. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
13. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
14. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
15. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).
16. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
17. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
18. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
19. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
20. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.

21. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
22. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
23. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
24. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
25. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
26. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
27. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
28. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
29. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
30. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
31. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
32. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiegś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.
33. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
34. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
35. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu.

36. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
37. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.
38. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
39. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
40. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
41. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
42. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
43. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
44. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
45. Funkcja generująca taki log ma oferować filtrowanie wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
46. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
47. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
48. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
49. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
50. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
51. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antyvirus, antyspyware, metody heurystyczne, zapora sieciowa).
52. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
53. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
54. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

55. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
56. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.
57. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.

Ochrona przed spamem

58. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
59. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
60. Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego.
61. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
62. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym.
63. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.
64. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.
65. Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci” obecnym w programie Microsoft Outlook.
66. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana” oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana”.
67. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall)

68. Zapora osobista ma pracować jednym z 4 trybów:
 - tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora
 - tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo),
 - tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,
 - tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji.

69. Program musi akceptować istniejące reguły w zaporze systemu Windows, zezwalające na ruch przychodzący
70. Możliwość tworzenia list sieci zaufanych.
71. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie
72. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
73. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.
74. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
75. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
76. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.
77. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
78. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
79. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci
80. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, konkretny interfejs sieciowy w systemie.
81. Program musi umożliwić ustalenie tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia.
82. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem.

Kontrola dostępu do stron internetowych

83. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.
84. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
85. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
86. Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
87. Moduł musi posiadać także możliwość grupowania kategorii już istniejących.
88. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj.
89. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny.

Ochrona serwera plików Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016, **2019**
2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
4. Wbudowana technologia do ochrony przed rootkitami i exploitami.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
8. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
9. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.
13. Aplikacja powinna wspierać mechanizm klastrowania.
14. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
15. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
16. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
17. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia.
18. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączonego urządzenia.
19. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
20. System antywirusowy ma automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
21. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
22. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
23. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
24. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
25. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
26. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.

27. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
28. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
29. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
30. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
31. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
32. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
33. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.
34. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
35. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
36. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
37. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
38. Funkcja generująca taki log ma oferować filtrowanie wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
39. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
40. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
41. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
42. Aplikacja musi wspierać skanowanie magazynu Hyper-V
43. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów
44. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).

45. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
46. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Administracja zdalna

1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012, 2016, **2019**
2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).
3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.
4. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.
5. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
6. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
7. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający co najmniej polski i angielski..
8. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
9. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
10. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
11. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny.
12. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
13. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
14. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
15. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
16. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
17. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
18. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.

19. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
20. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
21. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
22. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
23. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
24. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzeniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.
25. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
26. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
27. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
28. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
29. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
30. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
31. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
32. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
33. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
34. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
35. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stację kliencką.
36. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
37. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.

38. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.
39. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
40. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.
41. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
42. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
43. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.
44. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.
45. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
46. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
47. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
48. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
49. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.
50. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
51. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
52. Serwer administracyjny musi być wyposażona w mechanizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.
53. Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań.

Endpoint Detection and Response

Serwer

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych.
2. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
3. System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.
4. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego

- czyszczenia bazy danych.
6. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
 7. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
 8. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
 9. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
 10. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
 11. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
 12. Serwer musi posiadać ponad 800 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
 13. Serwer administracyjny musi posiadać możliwość uruchomienia reguł w oparciu o dane historyczne.
 14. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
 15. Serwer musi posiadać możliwość ustawiania priorytetu zdarzeń z użyciem 4-stopniowej skali.
 16. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
 17. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
 18. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
 19. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
 20. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
 21. Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie wprowadzonej nazwy.
 22. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
 23. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1

- pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal).
24. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
 25. Konsola administracyjna musi mieć możliwość tagowania obiektów.
 26. Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli.
 27. Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci.
 28. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
 29. Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł.

Agent

30. Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10, Windows 11 oraz Windows Server 2008/2012/2016/2019.
31. Pełne wsparcie dla systemów macOS 10.12 i nowszych.
32. Wsparcie dla 32 i 64-bitowej wersji systemu Windows.
33. Agent musi współpracować z produktem antywirusowym tego samego producenta.
34. Agent nie może działać bez produktu antywirusowego tego samego producenta.
35. W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonanej przez agenta.
36. Połączenie agenta do serwera zarządzającego musi być szyfrowane.
37. Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane.

W ramach pakietu dostawca przekaże licencje oraz zainstaluje na wskazanym serwerze oprogramowanie konsoli zarządzającej.