Opis przedmiotu zamówienia

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest zakup **dla 1553 użytkowników przedłużenia licencji**, posiadanej przez Zamawiającego, do oprogramowania antywirusowego ESET Endpoint Protection Advanced oraz zakup licencji **dla 453 nowych użytkowników** na okres:

- od 24 lipca 2020 r. do 23 lipca 2023 r.

wraz z pełną automatyczną subskrypcją aktualizacji baz wirusów i innych zagrożeń w tym okresie,

lub

zakup nowej licencji równoważnego oprogramowania antywirusowego **dla 2006 użytkowników** na okres:

- od 24 lipca 2020 do 23 lipca 2023,

wraz z pełną automatyczną subskrypcją aktualizacji baz wirusów i innych zagrożeń w tym okresie.

W przypadku zaoferowania oprogramowania równoważnego musi to być, to samo oprogramowanie dla obu pozycji zamówienia.

Wykonawca musi odinstalować posiadane przez Zamawiającego oprogramowania przed datą wygaśnięcia licencji i jednocześnie zainstalować, skonfigurować, aktywować i uruchomić dostarczone, równoważne oprogramowanie antywirusowe przed wymaganym terminem, z zastrzeżeniem, że okres licencjonowania musi obejmować czas od dnia aktywacji do 23 lipca 2023 r. Kompletne zadanie re-instalacji musi zostać wykonane maksymalnie do 5 dni roboczych w godzinach 8:00 – 15:00.

W przypadku odinstalowania istniejącego na komputerach Zamawiającego oprogramowania antywirusowego i instalacji dostarczanego oprogramowania antywirusowego, musi ono być aktywne i w pełni funkcjonalne w dniu jego instalacji.

II. OPIS I MINIMALNE TECHNICZNE, FUNKCJONALNE I UŻYTKOWE WYMAGANIA ZAMAWIAJĄCEGO DLA ROZWIĄZANIA RÓWNOWAŻNEGO:

1. Ochrona stacji roboczych - Windows

1) Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10.
2) Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3) Wersja programu dostępna co najmniej w języku polskim oraz angielskim.
4) Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim oraz angielskim.

2. Ochrona antywirusowa i antyspyware

1) Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

Opis przedmiotu zamówienia

2) Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
3) Wbudowana technologia do ochrony przed rootkitami.
4) Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5) Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6) Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie" lub według harmonogramu.
7) System ma posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
8) Skanowanie „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym systemu operacyjnego (min. Windows7, 8, 10).
9) Możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
10) Możliwość skanowania dysków sieciowych i dysków przenośnych.
11) Możliwość skanowania plików spakowanych i skompresowanych.
12) Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
13) Użytkownik musi posiadać możliwość tymczasowego wyłączenia.
14) Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
15) Oprogramowanie musi posiadać wbudowany konektor, min. dla programów MS Outlook, Windows Mail/Windows Live Mail.
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) Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
18) Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
19) Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
20) Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
21) Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
22) Wbudowane moduły heurystyczne: pasywne metody heurystyczne, aktywne metody heurystyczne oraz elementy sztucznej inteligencji.
23) Ewentualne dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

Opis przedmiotu zamówienia

24) Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
25) Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
26) 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 oraz urządzeń przenośnych.
27) Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
28) 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.
29) Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
30) Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
31) Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
32) Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
33) Program ma posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
34) Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
35) W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.
36) Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
37) Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron internetowych i kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
38) Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.

39) Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.
40) Możliwość podejrzenia informacji o licencji, która znajduje się w programie.
41) W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane.
42) Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
43) Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
44) Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
45) Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
46) Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
47) Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść".
48) Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
49) Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
50) Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
51) Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

3. Ochrona przed spamem

1) Ochrona antyspamowa dla programów pocztowych min. MS Outlook, Windows Mail/Windows Live Mail.
2) Wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
3) Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
4) Możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
5) Możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.

6) Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

4. Zapora osobista (personal firewall)

1) Zapora osobista ma pracować w min. jednym z czterech trybów:
   - tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
   - tryb interaktywny – program pyta się o każde nowo nawiązywane połączenie,
   - tryb oparty na regułach – program blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
   - tryb uczenia się – program automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
2) Możliwość tworzenia list sieci zaufanych.
3) Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
4) Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.
5) Możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
6) Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
7) Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
8) Wykrywanie modyfikacji w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.
9) Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
10) Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
11) 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, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.

5. Kontrola dostępu do stron internetowych

1) Aplikacja musi być wyposażona w zintegrowany moduł kontroli dostępu do stron internetowych.

2) Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory.
3) Aplikacja musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 100 kategorii i podkategorii.
4) 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.
5) Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych.
6) Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta.
7) Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
8) Aplikacja musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj.
9) Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej.

6. Stacje Robocze Apple Mac OS X

1) Pełne wsparcie dla systemów Mac OS X 10.9 lub nowszych.
2) Wersja programu dostępna co najmniej w języku polskim oraz angielskim.
3) Pomoc w programie (help) w języku polskim oraz angielskim.
4) Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
5) Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
6) Skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
7) Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8) Możliwość skanowania dysków sieciowych i dysków przenośnych.
9) Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
10) Ewentualne dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
11) Ochrona przed atakami typu „phishing”.

Opis przedmiotu zamówienia

12) Funkcja blokowania nośników wymiennych ma umożliwiać wyłączenie dostępu do nośników: Płyta CD/DVD, Pamięć masowa, Sieć, Drukarka USB, Urządzenie do tworzenia obrazów, Port szeregowy, Urządzenie przenośne.
13) Program umożliwia automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego.
14) Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania oraz dokonanym skanowaniem komputera.
15) Program musi posiadać mechanizm Ochrony dostępu do stron internetowych monitoruje komunikację w ramach protokołu HTTP.
16) Ochrona poczty mail:
    - Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej niezależnie od programu pocztowego.
    - 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).
    - Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
17) Zapora osobista. Zapora osobista może pracować jednym z 2 trybów:
    - Automatyczny z wyjątkami - umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł,
    - Interaktywny – dla każdej nieznanej komunikacji generowane jest pytanie dla użytkownika o jej odblokowanie.
    - Możliwość dezaktywacji funkcji zapory sieciowej.
    - Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
    - Możliwość odnotowania faktu nawiązania danego połączenia w dzienniku zdarzeń.
    - Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
    - Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
    - Aktywacja stref ma się odbywać min. w oparciu o: interfejs sieciowy w systemie, Sieć WiFi, Podsieć IPv4/IPv6, Zakres adresów IPv4/IPv6, Adres IPv4/IPv6.
18) Kontrola dostępu do stron internetowych
    - Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.
    - Aplikacja musi posiadać możliwość filtrowania URL w oparciu o co najmniej 100 kategorii i podkategorii.

- 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.
- Lista adresów URL, znajdujących się w poszczególnych kategoriach, musi być na bieżąco aktualizowana przez producenta.
- Użytkownik musi posiadać możliwość wyłączenia modułu kontroli dostępu do stron internetowych.

7. Stacje robocze Linux

1) Pełne wsparcie dla dystrybucji opartych na systemach min. Debian i RedHat (Ubuntu, OpenSuse, Fedora, Mandriva itp).
2) Wsparcie dla dystrybucji 32- i 64-bitowych.
3) Wersja programu dostępna zarówno w języku polskim jak i angielskim.
4) Pomoc w programie (help) w języku polskim.
5) Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
6) Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
7) Wbudowana technologia do ochrony przed rootkitami.
8) Skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
9) Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
10) Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
11) Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD oraz portów USB.
12) Program ma posiadać dwie wersje interfejsu (standardowy – z ukrytą częścią ustawień oraz zaawansowany – z widocznymi wszystkimi opcjami).
13) Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz sygnatur wirusów i samego oprogramowania oraz dokonanym skanowaniem komputera.

8. Ochrona urządzeń mobilnych opartych o system Android

1) Wspierany system co najmniej Android 5.0.
2) Rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa.
3) Procesor: ARM z obsługą ARMv7 lub x86 Intel Atom.

4) Ochrona plików w czasie rzeczywistym.
5) Ochrona przed atakami typu „phishing".
6) Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
7) Ochrona proaktywna wykrywająca nieznane zagrożenia.
8) W przypadku wykrycia zagrożenia użytkownik ma otrzymać odpowiednie powiadomienie.
9) Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji.
10) Informacje o skanowaniu mają być przechowywane w plikach dziennika.
11) Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania.
12) Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia.
13) W przypadku kradzieży urządzenia, Administrator ma mieć możliwość wysłania na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
    a) usunięcie zawartości urządzenia,
    b) przywrócenie urządzenie do ustawień fabrycznych,
    c) zablokowania urządzenia,
    d) uruchomienie sygnału dźwiękowego,
    e) lokalizację GPS.
14) Kontrola aplikacji:
    a) Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji.
    b) Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji.
15) Konfiguracja i zdalne zarządzanie:
    a) Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne.
    b) Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.
    c) Administrator musi mieć możliwość zdalnego wysyłania komunikatów z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych.
    d) Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna.

9. Ochrona serwera - Linux

1) Skaner antywirusowy i antyspyware.
2) Skanowanie plików, plików spakowanych i archiwów samorozpakowujących.
3) Oprogramowanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów oprogramowania, nie spowoduje to

przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

4) Oprogramowanie musi posiadać wbudowany mechanizm typu „watchdog". Monitoruje on tzw. stan zdrowia poszczególnych mikro-serwisów i automatycznie przeładowuje je w przypadku wykrycia zakłóceń w pracy mikro-serwisu.
5) Oprogramowanie antywirusowe musi wspierać wieloprocesorową i wielordzeniową architekturę, w celu zapewnienia maksymalnego zwiększenia wydajności.
6) Oprogramowanie antywirusowe musi być wyposażone w moduł ochrony systemu plików w czasie rzeczywistym. Moduł nie może wymagać instalowania jakichkolwiek dodatkowych komponentów w systemie operacyjnym. Wszystkie komponenty muszą być instalowane w systemie, podczas instalacji z dostarczonego instalatora binarnego.
7) Silnik ochrony systemu plików w czasie rzeczywistym musi stanowić dodatkowy moduł jądra systemu Linux i musi być dodawany do jądra, podczas procesu instalacji oprogramowania antywirusowego.
8) Ochrona systemu plików w czasie rzeczywistym musi być zapewniona nieprzerwanie od uruchomienia produktu i obejmuje skanowanie zarówno dysków lokalnych jak i zmapowanych dysków sieciowych.
9) Silnik skanujący musi działać wyłącznie z wykorzystaniem 64-bitowej architektury.
10) Oprogramowanie musi być w pełni zgodne z modułem SELinux, pracującym zarówno w trybie „Permissive" jak i „Enforcing".
11) Oprogramowanie podczas procesu instalacji, musi dodawać i konfigurować własne polityki modułu SELinux, które są kompatybilne z następującymi dystrybucjami systemów Linux: Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Centos 6, Centos 7.
12) Wszystkie mechanizmy bezpieczeństwa oprogramowania muszą wspierać system informowania o zagrożeniach w czasie rzeczywistym. System ten pozwala na weryfikowanie reputacji plików oraz procesów i identyfikację nowych i nieznanych zagrożeń.
13) Interfejs graficzny
    a) Produkt musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
    b) Lokalna konsola administracyjna musi działać w oparciu o dynamicznie generowaną zawartość (np. tworzoną z wykorzystaniem następujących technologii: React/Node.js, HTML5).
    c) Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
    d) Lokalna konsola administracyjna musi zapewniać bezpieczne połączenie działające w oparciu o protokół HTTPS.

e) Lokalna konsola administracyjna musi umożliwiać uruchomienie jej, na wskazanym porcie TCP.

14) Skanowanie sieciowych systemów plików: oprogramowanie antywirusowe musi pozwalać na skanowanie plików składowanych i obsługiwanych przez zewnętrzne rozwiązania obsługi danych typu NAS / SAN.

10. Ochrona serwera Windows

1) Wsparcie dla systemów: Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2008 R2 SP1, Microsoft Windows Server 2008 SP2 (oparty na procesorze x86 i x64), Server Core (Microsoft Windows Server 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016).
2) Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3) Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
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) Możliwość skanowania dysków sieciowych i dysków przenośnych.
9) Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
10) Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
11) Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
12) Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
13) Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
14) Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
15) 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 oraz urządzeń przenośnych.

16) W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
17) System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
18) Ewentualne dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
19) W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
20) 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.
21) Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
22) 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.
23) Aplikacja musi wspierać skanowanie magazynu Hyper-V.
24) Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów.
25) Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania.
26) Program musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”.
27) Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
28) Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
29) Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
30) Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
31) Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

11. Administracja zdalna

1) Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019 oraz systemach Linux.

Opis przedmiotu zamówienia

2) Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.
3) Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
4) Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.
5) Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
6) Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
7) Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.
8) Interfejs musi być zabezpieczony 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) Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
12) Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
13) Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi, host agenta wirtualnego.
14) Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.
15) Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
16) Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.
17) Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
18) Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.
19) Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.

Opis przedmiotu zamówienia

20) Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
21) Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.
22) Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
23) Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
24) Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.

25) Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
26) Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
27) Serwer administracyjny musi posiadać szablony raportów, przygotowanych przez producenta.
28) Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
29) Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
30) Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
31) Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
32) Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF, CSV oraz PS.
33) Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
34) Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.

Opis przedmiotu zamówienia

35) W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.
36) Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.