Lp.	Nazwa przedmiotu zamówienia	Ilość
1.	*SEP-NEW-S-AG-5K-10K-3Y Symantec Endpoint Protection, Initial Subscription License with Support, ACD-GOV 5,000-9,999 Devices 3 YR* Licencja ma obowiązywać od dnia zawarcia umowy (jednak nie wcześniej niż od dnia 01.01.2018 r.) do dnia 31.12.2020 r. *W ramach przedmiotu Zamawiający wymaga bezpłatnej pomoc techniczna świadczonej przez Wykonawcę (*telefonicznie w języku polskim (w godzinach od 8 do 17 od poniedziałku do piątek) i/lub angielskim (w pozostałych godzinach), internet (forum, email) całodobowa w języku angielskim).	5000 stanowisk

Wymagania Zamawiającego w przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego:

W wypadku zaoferowania oprogramowania równoważnego, Wykonawca odpowiedzialny jest za migracje istniejących centralnych konsol do zaoferowanego oprogramowania, migrację polityk (antywirusowych, wykluczeń, polityk zapory ogniowej, polityk kontroli aplikacji i urządzeń). Implementacja musi zostać udokumentowana dokumentem powdrożeniowym zawierającym: opis implementacji oraz procedury odzyskiwania całego środowiska, opis implementacji nowego środowiska, uwzględniający zachowanie poprzednich ustawień wprowadzonych w konsoli. Dodatkowo muszą zostać dostarczone procedury odzyskania sprawności działania systemu (w tym do odzyskania komunikacji pomiędzy klientem a serwerem) w przypadku niepowodzenia migracji do nowego systemu bezpieczeństwa. **Migracja środowiska Zamawiającego ma nastąpić w okresie wskazanym w rozdziale II ust. 4 SIWZ w zdaniu 2. W przypadku niepowodzenia procesu migracji Wykonawca zobowiązany jest przywrócić środowisko do stanu przed migracją oraz zapewnić ochronę Zamawiającego na aktualnych warunkach poprzez przedłużenie czasu trwania aktualnie funkcjonującego rozwiązania.**

Wykonawca ponosi również wszelkie możliwe koszty związane z wdrożeniem oferowanego oprogramowania, w szczególności koszty związane z odinstalowaniem bieżącego oprogramowania posiadanego przez Zamawiającego, koszty związane z przeszkoleniem min. 30 pracowników Zamawiającego (w tym dla min. 3 osób ma być przeprowadzone szkolenie certyfikowane, w zewnętrznej jednostce certyfikującej).

Szkolenie winno być przeprowadzone w terminie do 90 dni od daty zawarcia umowy, w terminie uzgodnionym z Zamawiajacym oraz winno obejmować co najmniej całe środowisko dydaktyczne tj. konsola + klienci, w wymiarze min. 2 dni roboczych po 8 godzin, obejmującego następujące zagadnienia:

1) Instalacja, migraja nowego oprogramowania bezpieczeństwa - omówienie opcji instalacyjnych. Omówienie instalacji i konfiguracji konsoli zarządzania.
2) Omówienie opcji oprogramowania antywirusowego i firewalla
3) Konfiguracja oprogramowania antywirusowego i firewalla
4) Wprowadzenie zmian w aplikacji i ich znaczenie dla ochrony
5) Testowanie bezpieczeństwa sieci z wprowadzonym rozwiązaniem ochronnym
6) Ochrona serwerów i konfiguracja oprogramowania w środowisku zwirtualizowanym
7) Konsola zarządzania - omówienie, wprowadzenie i migracja środowiska.

Termin realizacji zamówienia w przypadku zaoferowania oprogramowania obejmuje dostarczenie dokumentu potwierdzającego obowiązywanie licencji <u>oraz dokonanie wszystkich czynności związanych z wdrożeniem nowego oprogramowania (również odinstalowanie obecnie używanego oprogramowania przez Zamawiającego) itp., o których mowa powyżej (za wyjątkiem szkolenia, które winno zostać przeprowadzone w terminie do 90 dni od daty zawarcia umowy.</u>

Opis parametrów równoważności[1]:

I. Ochrona endpointa.

Ochrona antywirusowa:

- Usuwanie wirusów, makro–wirusów, robaków internetowych oraz koni trojańskich (oraz wirusów i robaków z plików skompresowanych oraz samorozpakowujących się) lub kasowanie zainfekowanych plików. Ochrona przed oprogramowaniem typu „spyware" i „adware", włącznie z usuwaniem zmian wprowadzonych do systemu przez to oprogramowanie tego typu.
- Wykrywanie wirusów, makro-wirusów, robaków internetowych, koni trojańskich, spyware, adware i dialerów i innego szkodliwego oprogramowania ma być realizowane w pojedynczym przebiegu skanowania.
- Optymalizacja wydajności ukierunkowana na zapewnienie dużej wydajności skanowania lub wydajności uruchomionych aplikacji,
- Skanowanie zaplanowane musi umożliwiać automatyczne pomijanie plików oraz folderów uznanych przez producenta i administratora systemów za zaufane
- Skanowanie plików pobranych z Internetu wraz ze skryptami umieszczonymi w sieci Internet oraz plików skompresowanych,
- Zapewnienie stałej ochrony wszystkich zapisywanych, odczytywanych, a także uruchamianych plików przez mechanizm skanujący pracujący w tle wraz z metodą heurystyczną wyszukiwania wirusów (na życzenie); pliki te mogą być skanowane:
  a) na dyskach twardych
  b) w boot sektorach
  c) na dyskietkach
  d) na płytach CD/DVD
  e) na zewnętrznych dyskach twardych (np. podłączonych przez port USB)
- Możliwość samodzielnego pobierania aktualizacji z Internetu do stacji roboczej
- Możliwość zablokowania funkcji zmiany konfiguracji klienta lub ukrycie interfejsu użytkownika klienta.
- Przekazywanie nieodwracalnie zainfekowanych plików do bezpiecznego miejsca w postaci centralnej kwarantanny na centralnym serwerze, w celu przeprowadzenia dalszych badań
- Wbudowana w oprogramowanie funkcja do wysyłania podejrzanych lub zainfekowanych nowymi wirusami plików do producenta w celu uzyskania szczepionek. System ma dawać możliwość wyłączenia niniejszej funkcji.
- Wyszukiwanie i usuwanie wirusów w plikach skompresowanych (także zagnieżdżonych wewnątrz innych plików skompresowanych) w szczególności z plikach typu ZIP, LZH/LHA, , ARJ, RAR, MIME/UU, TAR, kontenery CAB,UUE, ,
- Aktualizacja definicji wirusów nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie – serwerze czy stacji roboczej
- Mikrodefinicje wirusów - przyrostowe, scentralizowane aktualizowanie klientów jedynie o nowe definicje wirusów i mechanizmy skanujące
- Możliwość cofnięcia procesu aktualizacji definicji wirusów i mechanizmów skanujących – powrót do poprzedniego zastawu definicji wirusów bez konieczności deinstalacji oprogramowania czy też restartu komputerów

[1] W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego w stosunku do oprogramowania opisanego przez Zamawiającego w niniejszym dokumencie, oferowane oprogramowanie równoważne winno spełniać podane parametry równoważności, pod rygorem odrzucenia oferty.

- Możliwość natychmiastowego „wypchnięcia” definicji wirusów do stacji klienckich
- Aktualizacja bazy definicji wirusów oraz mechanizmów skanujących, co najmniej 3 razy dziennie
- Możliwość aktualizacji bazy definicji wirusów średnio, co 1 godzinę
- Heurystyczna technologia do wykrywania nowych, nieznanych wirusów
- moduł analizy w czasie rzeczywistym zachowań aplikacji do wykrywania nowych, nieznanych zagrożeń typu robak internetowy, koń trojański, keylogger – analiza zachowania opiera się na wykonywanych przez aplikację czynnościach (tworzenie nowych plików, komunikacja z internetem, podmiana strony w przeglądarce, itp.)
- moduł analizy w czasie rzeczywistym musi być aktualizowany niezależnie od ochrony antywirusowej poprzez konsolę zarządzającą lub ze stacji roboczej
- Automatyczna rejestracja w dzienniku zdarzeń wszelkich nieautoryzowanych prób zmian rejestru dokonywanych przez użytkownika.
- Automatyczne ponowne uruchomianie skanowania w czasie rzeczywistym, jeśli zostało wyłączone przez użytkownika mającego odpowiednie uprawnienia na z góry określony czas.
- Automatyczne wymuszanie na kliencie programu pobrania zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe
- Aktualizacje definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione
- Skanowanie poczty klienckiej (na komputerze klienckim)
- Opóźnienie skanowania zaplanowanego w wypadku działania komputera (laptopa) na bateriach
- Ściągnięcie dowolnego pliku na komputer musi spowodować sprawdzenie reputacji takiego pliku – jako reputacja rozumie się odpowiedź, co do ilość użytkowników w Internecie korzystających z danej aplikacji/pliku, czasu, kiedy aplikacja/plik pojawiła się w Internecie po raz pierwszy, oraz czy aplikacja/plik jest „dobra” czy też nie
- Produkt musi umożliwić utworzenie grup, które będą miały prawo uruchamiać ściągniętą aplikacje, jeżeli będzie z niej korzystać w Internecie zdefiniowana ilość użytkowników (przynajmniej: 5, 50, 100, setki użytkowników) oraz dana aplikacja będzie widziana w Internecie od określonej ilości dni
- W wypadku systemu Windows 8, wsparcie dla funkcji ELAM (Early Launch Anti-Malware)
- Dedykowany moduł wywoływany lokalnie lub zdalnie na żądanie z serwera zarządzającego wykonujący agresywne czynności naprawcze w przypadku infekcji na komputerze.
- Dla systemów typu Windows Embedded wsparcie dla Windows Embedded write filters w tym dla File-Based Write Filter (FBWF)
- Możliwość wyboru wielkości definicji antywirusowych, z której będzie korzystał zainstalowany agent – system musi posiadać pełna wersję sygnatur oraz ich wersję uproszczoną znacząco mniejszą od pełnej do instalacji na systemach z niewielką ilością miejsca na dyskach oraz w systemach VDI.
- System musi posiadać możliwość emulacji w celu analizy polimorficznego złośliwego oprogramowania.
- System musi być wyposażony w dynamiczny klasyfikator próbek wykorzystujący mechanizmy uczenia maszynowego (Machine Learning) w celu wykrywania nowych wersji znanych rodzin złośliwego oprogramowania. Zbiór danych wykorzystywany w algorytmach uczących musi pochodzić z sieci składającej się z co najmniej 150mln sond.

Zapora ogniowa – system Firewall

- Pełne zabezpieczenie stacji klienckich przed: atakami hakerów oraz nieautoryzowanymi próbami dostępu do komputerów i skanowaniem jego portów.
- Moduł firewall ma mieć możliwość monitorowania i kontroli, jakie aplikacje łączą się poprzez interfejsy sieciowe,
- Administrator może definiować połączenia, które stacja robocza może inicjować i odbierać,

- Administrator może konfigurować dostęp stacji do protokołów rozszerzonych innych niż ICMP,UDP czy TCP np.: IGMP, GRE, ,
- Program ma pozwalać na zdefiniowanie indywidualnych komputerów lub całych zakresów adresów IP, które są traktowane, jako: całkowicie bezpieczne lub niebezpieczne
- Program musi wykrywać próby wyszukiwania przez hakerów luk w zabezpieczeniach systemu w celu przejęcia nad nim kontroli
- Konfiguracja zezwalanego i zabronionego ruchu ma się odbywać w oparciu o takie informacje jak: interfejs sieciowy, protokół, stacja docelowa, aplikacja, godzina komunikacji
- Konfiguracja stacji ma się odbywać poprzez określenie: Adresu MAC, numeru IP, zakresu numerów IP, wskazanie podsieci, nazwy stacji DNS (FQDN) lub domeny DNS
- Firewall ma mieć konfigurowalną funkcjonalność powiadamiania użytkownika o zablokowanych aplikacjach
- Uniemożliwienie przejęcia sesji poprzez losowo generowane numery sekwencji TCP
- Domyślne reguły zezwalające na ruch DHCP, DNS, WINS
- Wsparcie dla protokołu IPv6

Ochrona przed włamaniami – system IPS

- Producent ma dostarczyć bibliotekę ataków i podatności (sygnatur) stosowanych przez produkt. Administrator ma mieć możliwość uaktualniania tej biblioteki poprzez konsolę zarządzającą oraz niezależnie, w postaci pliku exe, który można bezpośrednio uruchomić na kliencie.
- Biblioteka sygnatur musi zawierać również sygnatury dotyczące działalności programów P2P.
- Produkt ma mieć możliwość tworzenia własnych wzorców włamań (sygnatur), korzystając z semantyki Snort'a. Sygnatury te mogą działać w trybie blokuj lub rejestruj.
- Wykrywanie skanowania portów
- Ochrona przed atakami typu odmowa usług (Denial of Service)
- Blokowanie komunikacji ze stacjami z podmienionymi MAC adresami (spoofed MAC)
- Wykrywanie trojanów i generowanego przez nie ruchu
- Wykrywanie prób nawiązania komunikacji za pośrednictwem zaufanych aplikacji, przez inne oprogramowanie.
- Blokowanie komunikacji ze stacjami uznanymi za wrogie na zdefiniowany przez administratora czas. Ma istnieć możliwość definiowania wyjątków
- System ochrony przed włamaniami musi automatycznie integrować się z przeglądarką internetową (przynajmniej z Internet Explorer, EDGE, CHROME oraz Firefox) – uniemożliwiając wykonanie w nich (nawet, jeżeli są podatne) szkodliwego dla nich kodu
- System musi posiadać mechanizm blokowania wykorzystywania nieznanych podatności w określonym oprogramowaniu (Exploit Prevention) co najmniej dla aplikacji pakietu Office, Firefox, Internet Explorer oraz aplikacji napisanych w języku Java. System musi implementować co najmniej następujące metody prewencji:
    - Java Exploit Protection
    - Structured Exception Handling Overwrite Protection (SEHOP)
    - Heap Spray Memory Attack

Ochrona systemu operacyjnego

- Produkt ma umożliwiać uruchamianie i blokowanie wskazanych aplikacji
- Produkt ma umożliwiać ładownie modułów lub bibliotek DLL
- Produkt ma umożliwiać kontrolę odczytywania i zapisywania na systemie plików przez wskazane aplikacje

- Aplikacje powinny być rozróżniane poprzez nazwę i sygnaturę cyfrową
- Produkt ma umożliwiać blokowanie wskazanego typu urządzeń przed dostępem użytkownika – urządzenia muszą być identyfikowane po ich numerze seryjnym
- Produkt ma kontrolować dostęp do rejestru systemowego
- Produkt ma umożliwiać logowanie plików wgrywanych na urządzenia zewnętrzne
- Produkt musi automatycznie umożliwić zablokowanie pliku autorun.inf na urządzeniach zewnętrznych i na udziałach sieciowych
- Polityki ochrony mają mieć możliwość pracy w dwóch trybach, testowym i produkcyjnym. W trybie testowym aplikacje i urządzenia nie są blokowane, ale jest tworzony wpis w logu
- Możliwość wykluczenia dowolnej aplikacji z trybu ochrony systemu operacyjnego
- Możliwość utworzenie listy zaufanych aplikacji (tzw. białej listy) i konfiguracji produktu w taki sposób, by żadna inna aplikacja/biblioteka z poza listy nie mogła uruchomić się na komputerze
- Kolekcja aktualnie znajdujących się aplikacji na systemie końcowym musi być możliwa do wywołania bezpośrednio z konsoli zarządzającej – bez konieczności wykonania jakichkolwiek czynności na systemie końcowym
- Możliwość utworzenia listy blokowanych aplikacji (tzw. czarnej listy) i konfiguracji produktu w taki sposób, by tylko aplikacja znajdujące się na liście nie mogły uruchomić się na komputerze
- Możliwość automatycznego importu list zarówno białej, jaki i czarnej, co zdefiniowany interwał czasu

Integralności komputera:

- Oprogramowanie musi umożliwiać wykonywanie szerokiego zakresu testów integralności komputera pod kątem zgodności z polityką bezpieczeństwa urządzeń końcowych, w tym: programów antywirusowych, poprawki firmy Microsoft, dodatki Service Pack firmy Microsoft, osobistych zapór ogniowych
- Testy integralności ma być przeprowadzany cyklicznie, co zdefiniowany okres czasu.
- Powyższe szablony muszą być automatycznie aktualizowane ze strony producenta
- Oprogramowanie musi umożliwiać wykonanie niestandardowego (dowolnie zdefiniowanego) testu integralności komputera, posiadać zaawansowaną składnie If…Then…Else.
- W przypadku niestandardowego testu integralności musi istnieć dostępność następujących testów:
  a) Wpisy rejestru systemu operacyjnego - istnienie, określona wartość, inne
  b) Pliki - istnienie, data, rozmiar, suma kontrolna
  c) Wiek, data, rozmiar pliku sygnatury oprogramowania antywirusowego
  d) Zainstalowane poprawki
  e) Uruchomiony proces, wersja systemu operacyjnego
  f) Własny skrypt VisualBasic, wsh, itp.
  g) Własna aplikacja
- W przypadku niezgodności stacji z testem integralności, musi być możliwość ustawienia akcji naprawczej na poziomie pojedynczego testu. Jako możliwe operacje do wykonania, musi istnieć możliwość:
  a) Uruchamianie dowolnego/własnego skryptu lub programu
  b) Logowanie zdarzenia
  c) Ukazanie okienka z wiadomością
  d) Pobieranie oraz uruchamianie instalacji
- Ma istnieć możliwość wskazania czasu oczekiwania na wykonanie akcji naprawczych.
- Możliwość wymuszenia instalacji dowolnej aplikacji.

- W wypadku niezgodności własnego systemu, oprogramowanie musi umożliwić zaaplikowanie dowolnego innego zestawu konfiguracji, w szczególności polityki firewallowej (zdefiniowanej bardzo restrykcyjnie), polityki antywirusowej, polityki pobierania aktualizacji, polityki kontroli uruchamianych aplikacji i polityki kontroli urządzeń.
- Musi być możliwe, nieuwzględnianie wyniku poszczególnego testu na wynik końcowy integralności komputera.
- Musi istnieć możliwość stwierdzenia, że na komputerze znaleziono zagrożenie i nie można było takiego zagrożenia usunąć – na ten czas komputer powinien znaleźć się w kwarantannie.
- Musi istnieć test integralności komputera, który sprawdzi czy komputer nie jest podłączony do Internetu poprzez dwie różne drogi, np. poprzez kabel sieciowy (Ethernet) i poprzez dostęp mobilny (WIFI, modem GSM, etc.)

Ochrona środowisk wirtualnych

- Produkt musi umożliwiać identyfikacje środowiska wirtualnego, w którym działa, informacja na ten temat musi być widoczna w konsoli. Minimalnie identyfikowane środowiska to: Citrix, Microsoft, VMWare
- Produkt musi umożliwiać w wypadku skanowania w czasie rzeczywistym oraz przy skanowaniu zaplanowanym, wykluczenie w środowisku wirtualnym wszystkich plików z tzw. złotego obrazu (Gold Image) - nie będą one nigdy poddawane skanowaniu
- Produkt musi umożliwiać współdzielenie wyników skanowania zaplanowanego i na żądanie pomiędzy instancjami wirtualnymi - znalezienie już raz przeskanowanego tego samego pliku powoduje nieskanowanie go na systemie pytającym. Technologia ta powinna być dostępna, jako oprogramowanie instalowane w systemie operacyjnym Windows
- Produkt musi umożliwiać prawidłowe rozliczenia licencji oferowanego systemu dla systemów wirtualnych typu desktop tzw. VDI, w szczególności tzw. „non-persistent”
- Produkt musi umożliwiać przeskanowanie plików vmdk w poszukiwaniu zagrożeń

Architektura

- Rozwiązanie ma mieć architekturę trój-warstwową. Klienci mają być zarządzani przez serwery, a konfiguracja rozwiązania ma być zapewniona poprzez graficzną konsolę administratora.
- Rozwiązanie ma zapewniać wysoką skalowalność i odporność na awarie.
- Komunikacja pomiędzy agentami i serwerem ma być szyfrowana.
- Numery portów używane do komunikacji mają mieć możliwość konfiguracji przez użytkownika końcowego.
- Agent ma się przełączać do innego serwera zarządzającego w przypadku niedostępności przypisanego serwera.
- Serwery zarządzające mają móc replikować pomiędzy sobą informacje o agentach, ich konfiguracji oraz logi. Musi istnieć możliwość zdefiniowania kierunku replikacji logów (jednostronna lub dwustronna).
- Musi istnieć możliwość zdefiniowania dowolnego klienta, jako lokalnego dostarczyciela aktualizacji – możliwość konfiguracji ilości przetrzymywanych aktualizacji, zajętości na dysku oraz konfiguracji prędkości ich pobierania z serwera zarządzającego.
- Definiowanie lokalnego repozytorium musi zawierać warunki, jakie muszą być zachowane by dany komputer mógł stać się lokalnym repozytorium – warunkami muszą być przynajmniej: wersja systemu operacyjnego, adres komputera, nazwa komputera (z możliwością podania ją ze znakami specjalnymi, np.: komputer*), określonego wpisu w rejestrze.
- Możliwość manualnego wskazania wybranej grupie komputerów konkretnego lokalnego dostarczyciela aktualizacji.

- Możliwość uruchomienia dedykowanego narzędzia służącego do monitorowania klientów, którzy zostali lokalnymi dostarczycielami aktualizacji. Monitorowane jest ich zdrowie, ilość ściągniętych od nich danych, czy były to ściągnięte pełne definicje czy też definicje przyrostowe.
- Możliwość ograniczenia pasma sieciowego od serwera zarządzającego do jego klientów w zależności od ściąganych definicji, aktualizacji klienckiej, podsieci, z której się łączą.

Moduł raportujący:

- Produkt ma zapewniać graficzne raportowanie,
- Wbudowane raporty maja pokazywać:
  a) stan dystrybucji sygnatur antywirusowych, sygnatur heurystycznych oraz IDS/IPS
  b) wersje zainstalowanych klientów
  c) inwentaryzacje stacji roboczych (w tym wielkość dysku, zajętość dysku, wielkość pamięci RAM, wykorzystywany system operacyjny oraz procesor)
  d) wykrytych wirusów, zdarzeń sieciowych, integralności komputerów
  e) zainstalowane technologie i ich aktualny stan
- Moduł raportowania ma pokazywać stan wykonywanych poleceń na komputerach
- Możliwość zaplanowanego tworzenia raportów i przesyłania ich do danych kont pocztowych
- Produkt musi umożliwiać automatyczne zbudowanie zapytań, które będą wykonywane o zdanym czasie i ich wynik będzie przechowywany w postacie kostek OLAP. Powstałe kostki muszą umożliwiać wykonywanie na nich typowych operacji takich jak zwijanie/agregacja danych, rozwijanie (bardziej szczegółowe dane), selekcja (wybór intersujących danych). Wszystkie te operacje muszą być wykonywane graficznie.
- Produkt musi umożliwiać automatyczne budowanie trendów
- Produkt musi umożliwiać automatyczne budowanie kluczowych wskaźników wydajności (KPI)

Moduł centralnego zarządzania:

- Centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem z pojedynczej konsoli
- Centralna aktualizacja ochrony antywirusowej, zapory ogniowej i systemu wykrywania włamań przez administratora sieci,
- Produkt ma wykrywać i raportować nieautoryzowane zmiany w konfiguracji produktu na stacji roboczej. Ma istnieć możliwość blokowania takich zmian.
- Produkt ma zapewniać zarządzanie poprzez konsolę. Dostęp do konsoli ma być możliwy po wcześniejszej weryfikacji użytkownika. Produkt ma mieć możliwość definiowania wielu kont administracyjnych i niezależną konfigurację uprawnień.
- Możliwość definiowania wielu niezależnych organizacji na jednym serwerze zarządzającym – informacje dostarczone do serwera zarządzającego nie będą dostępne pomiędzy organizacjami
- Integracja z Microsoft Active Directory w celu importu użytkowników, listy maszyn, struktury jednostek organizacyjnych.
- Konta administracyjne mają być tworzone na poziomie serwerów zarządzających i na poziomie organizacji definiowanych na serwerze.
- Uprawnienia administratorów mają być ustawiane niezależnie dla każdego kontenera wewnątrz organizacji.
- Możliwość utworzenia administratorów z uprawnieniami tylko do odczytu.
- Konfiguracja agentów ma mieć strukturę drzewa, z mechanizmami dziedziczenia.
- Uwierzytelnianie administratorów ma się odbywać w oparciu o wewnętrzną bazę danych lub z użyciem Microsoft Active Directory. Produkt ma mieć możliwość wykorzystania wielo-elementowego uwierzytelniania (np. z wykorzystaniem tokenów, certyfikatów itp.)

- Dostęp do interfejsu produktu i listy funkcji dostępnych dla użytkownika ma być konfigurowany z poziomu centralnej konsoli zarządzającej.
- Konfiguracja aktywna na stacji ma rozróżniać lokalizację agenta i według tego kryterium określać stosowany zestaw reguł/polityk dla agenta.
- Lokalizacja ma być określana według istnienia lub nieistnienia: typu interfejsu sieciowego, numeru MAC domyślnej bramki, adresu IP, zakresu podsieci, wartości kluczy w rejestrze, komunikacji z serwerem zarządzającym, nazwy domeny, adresów serwerów WINS, DNS, DHCP, wyniku zapytania do serwera DNS.
- Opis lokalizacji powinien zawierać możliwość tworzenia połączeń logicznych „I" oraz „LUB" na powyżej wymienionych elementach.
- Paczki instalacyjne produktu mają pozwalać na dodanie własnej konfiguracji
- W paczce instalacyjnej musi być zawarta funkcjonalność deinstalacji innych produktów bezpieczeństwa, która uruchomi się automatycznie przed instalacją produktu
- Pełna funkcjonalność ma być zawarta w jednym pliku instalacyjnym
- Nowe wersje oprogramowania mają być automatycznie dystrybuowane na stacje robocze w postaci różnicy między aktualnie zainstalowaną wersją na kliencie a nową wersją oprogramowania.
- Produkt ma automatycznie wykrywać wszystkie urządzenia przyłączone do sieci komputerowej.
- Możliwość zdefiniowania alertów administracyjnych zawierających zdarzenia:
  a) błędnej autoryzacji do systemu zarządzania
  b) dostępności nowego oprogramowania
  c) pojawienia się nowego komputera
  d) zdarzeń powiązanych z infekcjami wirusów
  e) stanu serwerów zarządzających
- Możliwość konfiguracji przepustowości pasma pomiędzy klientami a serwerem zarządzającym osobna dla pobieranych definicji przyrostowych, pełnych i pakietów aktualizacji
- Oficjalna dokumentacja schematu bazy danych, z której korzysta system zarządzający
- Pełna polska wersja językowa oprogramowania dla systemu zarządzania i stacji klienckich wraz z dokumentacją.

Platforma:

- Oprogramowanie musi działać na systemach
  - Windows Vista (32-bit, 64-bit)
  - Windows 7 (32-bit, 64-bit; RTM and SP1)
  - Windows Embedded 7 Standard, POSReady, and Enterprise (32-bit and 64-bit)
  - Windows 8 (32-bit, 64-bit)
  - Windows Embedded 8 Standard (32-bit and 64-bit)
  - Windows 8.1 (32-bit, 64-bit), including Windows To Go
  - Windows 8.1 update for April 2014 (32-bit, 64-bit)
  - Windows 8.1 update for August 2014 (32-bit, 64-bit)
  - Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (32-bit and 64-bit)
  - Windows 10 (32-bit, 64-bit; RTM, November Update (2015), and Anniversary Update)
  - Windows Server 2008 (32-bit, 64-bit; R2, SP1, and SP2)
  - Windows Small Business Server 2008 (64-bit)
  - Windows Essential Business Server 2008 (64-bit)
  - Windows Small Business Server 2011 (64-bit)
  - Windows Server 2012
  - Windows Server 2012 R2

    - Windows Server 2012 R2 update for April 2014
    - Windows Server 2012 R2 update for August 2014
    - Windows Server 2016
- Komponenty rozwiązania takie jak: firewall, zapobieganie włamaniom, kontrola urządzeń i aplikacji oraz kontrola integralności komputera muszą działać na wszystkich powyższych platformach 32 i 64-bitowych.
- Serwer zarządzający musi działać na systemach:
    - Windows Server 2008 (64-bit)
    - Windows Server 2008 R2
    - Windows Server 2012
    - Windows Server 2012 R2
    - Windows Server 2016

Ochrona antywirusowa dla systemu Macintosh

- Ochrona antywirusowa (z pominięciem funkcji reputacji), system IPS oraz blokada urządzeń ma działać na platformie Mac OS X 10.9, 10.10, 10.11, oraz macOS 10.12.
- Klient dla system Mac ma być zarządzany przez ten sam serwer oraz z tej samej konsoli zarządzającej, co klienci Windows.

Ochrona antywirusowa dla systemu Linux

- Ochrona antywirusowa z pominięciem funkcji reputacji ma działać na platformie:
    - CentOS 6U4, 6U5; 32-bit and 64-bit
    - Debian 6.0.5 Squeeze, Debian 8 Jessie; 32-bit and 64-bit
    - Fedora 16, 17; 32-bit and 64-bit
    - Oracle Linux (OEL) 6U2, 6U4, 6U5, 7
    - Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U8, 7, 7.1, 7.2
    - SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP3, 32-bit and 64-bit; 12
    - SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP3; 32-bit and 64-bit
    - Ubuntu 12.04, 14.04, 16.04; 32-bit and 64-bit
- Klient dla system Linux ma być zarządzany przez ten sam serwer oraz z tej samej konsoli zarządzającej, co klienci Windows.