Załącznik nr 1 do SIWZ

Opis równoważności oprogramowania antywirusowego

W przypadku zaoferowania oprogramowania innego niż Symantec Endpoint Protection 14.3 (lub najnowszej wersji), oferowane oprogramowanie powinno być oprogramowaniem równoważnym , przez które Zamawiający rozumie oprogramowanie zapewniające co najmniej poniższe funkcjonalności:

1) 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 ma być realizowane w pojedynczym systemie skanującym.
- Określanie obciążenia CPU dla zadań skanowania zaplanowanego oraz skanowania na żądanie,
- Skanowanie zaplanowane musi umożliwiać automatyczne pomijanie plików uznanych przez producenta 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 płytach CD/DVD
  d) 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.
- Wyszukiwanie i usuwanie wirusów w plikach skompresowanych (także zagnieżdżonych wewnątrz innych plików skompresowanych) w szczególności z plikach typu ZIP, GNU, LZH/LHA, BinHex, ARJ, RAR, MIME/UU, TAR, kontenery CAB,UUE, Rich Text Format,
- 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
- Możliwość natychmiastowego wymuszenia aktualizacji definicji wirusów na stacjach klienckich i serwerach.
- Aktualizacja bazy definicji wirusów oraz mechanizmów skanujących, co najmniej 3 razy dziennie
- Aktualizacja baz definicji musi być aplikowana tylko w czasie nieaktywności użytkownika na komputerze – jeżeli użytkownik komputera na nim pracuje, aplikacja automatycznie zostaje opóźniona
- Heurystyczna technologia do wykrywania nowych, nieznanych wirusów
- Dedykowany 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.). Schematy szkodliwego działania powinny być generowane w procesie uczenia maszynowego (Machine Learning) zaimplementowanego na sieci składającej się z co najmniej 150 milionów sond.
- 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,
- W Windows 8 i Windows 10 wsparcie dla funkcji ELAM (Early Launch Anti-Malware) poprzez dostarczenie odpowiedniego sterownika ELAM.
- Dedykowany moduł wywoływany lokalnie lub zdalnie na żądanie z serwera zarządzającego wykonujący agresywne czynności naprawcze w przypadku infekcji na komputerze.
- 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.

2) 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, VISA, OSPFIGP, L2TP, Lite-UDP,
- 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
- Firewall ma mieć konfigurowalną funkcjonalność powiadamiania użytkownika o zablokowanych aplikacjach. Ma istnieć możliwość dodania własnego komunikatu.
- W przypadku wykrycia zdefiniowanego ruchu, firewall ma wysłać wiadomość do administratora
- Uniemożliwianie określenia systemu operacyjnego i rodzaju przeglądarki internetowej przez serwery www
- Uniemożliwienie określenia systemu operacyjnego poprzez analizę pakietów sieciowych wysyłanych przez stację
- Uniemożliwienie przejęcia sesji poprzez losowo generowane numery sekwencji TCP
- Domyślne reguły zezwalające na ruch DHCP, DNS, WINS

3) Ochrona przed włamaniami – system IPS

- Biblioteka ataków i podatności musi zawierać przynajmniej 4500 sygnatur.
- 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 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 a także VLC. System musi implementować co najmniej 10 technik ochrony w tym następujące metody prewencji:
- (Java Exploit Protection, Structured Exception Handling Overwrite Protection (SEHOP), Heap Spray Memory Attack, Forced DEP, Forced ASLR, Anti-ROP)

4) Ochrona systemu operacyjnego

- Produkt ma umożliwiać uruchamianie i blokowanie wskazanych aplikacji
- 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
- 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
- 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

5) 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.
- 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 ograniczenia pasma sieciowego od serwera zarządzającego do jego klientów w zależności od ściąganych definicji, aktualizacji klienckiej, podsieci, z której się łączą.

6) 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

7) 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
- 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.
- Dostęp do interfejsu produktu i listy funkcji dostępnych dla użytkownika ma być konfigurowany z poziomu centralnej konsoli zarządzającej.
- 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) dostępności nowego oprogramowania
  b) pojawienia się nowego komputera
  c) zdarzeń powiązanych z infekcjami wirusów
  d) stanu serwerów zarządzających
- Możliwość konfiguracji przepustowości pasma pomiędzy klientami a serwerem zarządzającym osobna dla pobieranych definicji przyrostowych, pełnych i pakietów aktualizacji
- Pełna polska wersja językowa oprogramowania dla systemu zarządzania i stacji klienckich wraz z dokumentacją.

8) Oprogramowanie klienckie musi działać na systemach :

- Windows 7 (32-bit, 64-bit; SP1) Enterprise (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit)
- Windows 10 (32-bit, 64-bit;)
- Windows Server 2008 (32-bit, 64-bit;)
- Windows Server 2012
- Windows Server 2012 R2
- 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.

9) 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

10) Ochrona antywirusowa dla systemu Linux:

- Ochrona antywirusowa z pominięciem funkcji reputacji ma działać na platformie:
- Debian 6.0.5 Squeeze, Debian 8 Jessie; 32-bit and 64-bit
- Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U8, 7, 7.1, 7.2
- 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.