

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest zakup licencji na oprogramowanie antywirusowe zgodnie z okresami ważności licencji opisanymi w pkt. 1. oraz wymaganiami technicznymi zawartymi w pkt. 2. Zamawiający dopuszcza oferowanie produktu równoważnego, spełniającego warunki techniczne wymienione w pkt. 2 niniejszego Opisu przedmiotu zamówienia.

- 1) Zamawiający wymaga aby wykonawca wyrównał bieg posiadanych przez Zamawiającego licencji na oprogramowanie Symantec Protection Suite Enterprise Edition 3.0 do daty 27 grudnia 2011. Okres ważności poszczególnych licencji przedstawiony jest poniżej w tabelach.

Lp.	Nazwa	Ilość
1	Odnowienie posiadanych licencji Symantec Protection Suite Enterprise Edition 3.0 Basic GOV	210 szt.

Customer Number: 56207008.

Renewal ID: RNW529-831-600.

- a) Okres ważności pierwszego pakietu licencji:

Product Description	Qty	Expiry date	Renewal SKU to purchase is	Renewal SKU Desc
SYMC PROTECTION SUITE ENTERPRISE EDITION 3.0 PER USER BNDL STD LIC BASIC 12 MONTHS GOV BAND A	160	21.10.2010	20016675	SYMC PROTECTION SUITE ENTERPRISE EDITION 3.0 PER USER RENEWAL BASIC 12 MONTHS GOV BAND A

- b) Okres ważności drugiego pakietu licencji:

Product Description	Qty	Expiry date	Renewal SKU to purchase is	Renewal SKU Desc
SYMC PROTECTION SUITE ENTERPRISE EDITION 3.0 PER USER BNDL STD LIC BASIC 12 MONTHS GOV BAND A	50	27.12.2010	20016675	SYMC PROTECTION SUITE ENTERPRISE EDITION 3.0 PER USER RENEWAL BASIC 12 MONTHS GOV BAND A

- 2) Wymagania techniczne dla programu równoważnego z SYMANTEC PROTECTION SUITE ADVANCED BUSINESS EDITION 3.0 (serwery, stacje robocze, serwer poczty elektronicznej Exchange):

I Ochrona komputerów i serwerów (Endpoint)

1. Antywirus

- 1.1. 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.
- 1.2. Wykrywanie wirusów, makro-wirusów, robaków internetowych, koni trojańskich, spyware, adware i dialerów ma być realizowane w pojedynczym systemie skanującym. 3. Określanie obciążenia CPU dla zadań skanowania zaplanowanego oraz skanowania na żądanie.
- 1.3. Skanowanie plików pobranych z Internetu wraz ze skryptami umieszczonymi w sieci Internet oraz plików skompresowanych.
- 1.4. 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:
 - na dyskach twardych,
 - w boot sektorach,
 - na dyskietkach,
 - na płytach CD/DVD.
- 1.5. Możliwość samodzielnej pobierania aktualizacji z Internetu do stacji roboczej.
- 1.6. Możliwość zablokowania funkcji zmiany konfiguracji klienta lub ukrycie interfejsu użytkownika klienta.
- 1.7. Scentralizowana obsługa wirusów polegająca na przekazywaniu nieodwracalnie zainfekowanych plików do bezpiecznego miejsca w postaci centralnej kwarantanny na centralnym serwerze, w celu przeprowadzenia dalszych badań.
- 1.8. Wbudowana w oprogramowanie funkcja do wysyłania podejrzanych lub zainfekowanych nowymi wirusami plików do producenta w celu uzyskania szczepionek.
- 1.9. Wyszukiwanie i usuwanie wirusów w plikach skompresowanych (także zagnieżdżonych wewnątrz innych plików skompresowanych) w szczególności z plikach typu ZIP, GNU, LZH/LHA, BinHex, HTTP, ARJ, RAR, MIME/UU, TAR, kontenery CAB,UUE, Rich text format, ArcManager, MS-TNEF.
- 1.10. Aktualizacja definicji wirusów nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie – serwerze czy stacji roboczej.
- 1.11. Mikrodefinicje wirusów - przyrostowe, scentralizowane aktualizowanie klientów jedynie o nowe definicje wirusów i mechanizmy skanujące.
- 1.12. Możliwość cofnięcia procesu aktualizacji definicji wirusów i mechanizmów skanujących – powrót do poprzedniego zestawu definicji wirusów bez konieczności reinstalacji oprogramowania czy też restartu komputerów.

- 1.13. Możliwość natychmiastowego „wypchnięcia” definicji wirusów do stacji klienckich.
- 1.14. Aktualizacja bazy definicji wirusów oraz mechanizmów skanujących co najmniej 1 raz dziennie.
- 1.15. Możliwość aktualizacji bazy definicji wirusów średnio co 1 godzinę.
- 1.16. Heurystyczna technologia do wykrywania nowych, nieznanymi wirusów.
- 1.17. Moduł analizy zachowań aplikacji do wykrywania nowych, nieznanymi zagrożeń typu robak internetowy, koń trojański, keylogger.
- 1.18. Automatyczna rejestracja w dzienniku zdarzeń wszelkich nieautoryzowanych prób zmian rejestru dokonywanych przez użytkownika.
- 1.19. Automatyczne ponowne uruchomienie skanowania w czasie rzeczywistym, jeśli zostało wyłączone przez użytkownika mającego odpowiednie uprawnienia na z góry określony czas.
- 1.20. Automatyczne wymuszanie na kliencie programu pobrania zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe.
- 1.21. Aktualizacje definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
- 1.22. Skanowanie poczty klienckiej (na komputerze klienckim).
- 1.23. Opóźnienie skanowania zaplanowanego w wypadku działania komputera (laptopa) na bateriach.

2. Firewall

- 1.1. Opóźnienie skanowania zaplanowanego w wypadku działania komputera (laptopa) na bateriach.
- 1.2. Pełne zabezpieczenie stacji klienckich przed: atakami hakerów oraz nieautoryzowanymi próbami dostępu do komputerów i skanowaniem portów.
- 1.3. Moduł firewalla ma mieć możliwość monitorowania i kontroli, jakie aplikacje łączą się poprzez interfejsy sieciowe.
- 1.4. Administrator może definiować połączenia, które stacja robocza może inicjować i odbierać.
- 1.5. Administrator może konfigurować dostęp stacji do protokołów rozszerzonych innych niż ICMP, UDP czy TCP np.: IGMP, GRE, VISA, OSPFIGP, L2TP, Lite-UDP.
- 1.6. Aktualizacje definicji sygnatur ataków posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
- 1.7. Program ma pozwalać na zdefiniowanie indywidualnych komputerów lub całych zakresów adresów IP, które są traktowane jako: całkowicie bezpieczne lub niebezpieczne.
- 1.8. Program musi wykrywać próby wyszukiwania przez hakerów luk w zabezpieczeniach systemu w celu przejęcia nad nim kontroli.
- 1.9. Konfiguracja zezwalanego i zabronionego ruchu ma się odbywać w oparciu o takie informacje jak: interfejs sieciowy, protokół, stacja docelowa, aplikacja, godzina komunikacji.
- 1.10. Konfiguracja stacji ma się odbywać poprzez określenie: Adresu MAC, numeru IP, zakresu numerów IP, wskazanie podsieci, nazwy stacji dns (FQDN) lub domeny dns.
- 1.11. 10. Firewall powinien umożliwiać nagrywanie komunikacji spełniającej wskazane wymagania.

- 1.12. Firewall ma mieć konfigurowalną funkcjonalność powiadamiania użytkownika o zablokowanych aplikacjach. Ma istnieć możliwość dodania własnego komunikatu.
- 1.13. W przypadku wykrycia zdefiniowanego ruchu, firewall ma wysłać wiadomość do administratora.
- 1.14. Uniemożliwienie określenia systemu operacyjnego i rodzaju przeglądarki internetowej przez serwery WWW.
- 1.15. Uniemożliwienie określenia systemu operacyjnego poprzez analizę pakietów sieciowych wysyłanych przez stację.
- 1.16. Uniemożliwienie przejęcia sesji poprzez losowo generowane numery sekwencji TCP.
- 1.17. Domyślne reguły zezwalające na ruch DHCP, DNS, WINS.

3. Ochrona przed włamaniami

- 1.1. Producent ma dostarczyć bibliotekę ataków i podatności (sygnatur) stosowanych przez produkt. Administrator ma mieć możliwość uaktualniania tej biblioteki poprzez konsolę zarządzającą.
- 1.2. Produkt ma mieć możliwość tworzenia własnych wzorców włamań (sygnatur), korzystając z semantyki Snort'a.
- 1.3. Wykrywanie skanowania portów.
- 1.4. Ochrona przed atakami typu odmowa usług (Denial of Service).
- 1.5. Blokowanie komunikacji ze stacjami z podmienionymi MAC adresami (spoofed MAC).
- 1.6. Wykrywanie trojanów i generowanego przez nie ruchu.
- 1.7. Wykrywanie prób nawiązania komunikacji za pośrednictwem zaufanych aplikacji, przez inne oprogramowanie.
- 1.8. Blokowanie komunikacji ze stacjami uznanymi za wrogie na zdefiniowany przez administratora czas. Ma istnieć możliwość definiowania wyjątków.
- 1.9. System IDS/IPS ma umożliwiać nagrywanie komunikacji (zawartości pakietów przesyłanych w tej samej sesji) spełniającej wymagania określone we własnej (stworzonej przez administratora) sygnaturze IPS/IDS.

4. Ochrona systemu operacyjnego

- 1.1. Produkt ma umożliwiać uruchamianie i blokowanie wskazanych aplikacji.
- 1.2. Produkt ma umożliwiać ładowanie modułów lub bibliotek DLL.
- 1.3. Produkt ma umożliwiać kontrolę odczytywania i zapisywania na systemie plików przez wskazane aplikacje.
- 1.4. Aplikacje powinny być rozróżniane poprzez nazwę i sygnaturę cyfrową.
- 1.5. Produkt ma umożliwiać blokowanie wskazanego typu urządzeń przed dostępem użytkownika – urządzenia muszą być identyfikowane po ich numerze seryjnym.
- 1.6. Produkt ma kontrolować dostęp do rejestru systemowego.
- 1.7. Produkt ma umożliwiać logowanie plików wgrzywanych na urządzenia zewnętrzne.
- 1.8. 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.

5. Architektura

- 1.1. Rozwiązanie ma mieć architekturę trój-warstwową. Klienci mają być zarządzani przez serwery, a konfiguracja rozwiązania ma być zapewniona poprzez graficzną konsolę administratora.
- 1.2. Rozwiązanie ma zapewniać wysoką skalowalność i odporność na awarie.
- 1.3. Komunikacja pomiędzy agentami i serwerem ma być szyfrowana.
- 1.4. Numery portów używane do komunikacji mają mieć możliwość konfiguracji przez użytkownika końcowego.
- 1.5. Agent ma się przełączać do innego serwera zarządzającego w przypadku niedostępności przypisanego serwera.
- 1.6. Serwery zarządzające mają móc replikować pomiędzy sobą informacje o agentach, ich konfiguracji oraz logi. Musi istnieć możliwość zdefiniowania kierunku replikacji logów (jednostronna lub dwustronna).
- 1.7. Musi istnieć możliwość zdefiniowania dowolnego klienta jako lokalnego dostawcy aktualizacji – możliwość konfiguracji ilości przetrzymywanych aktualizacji, zajętości na dysku oraz konfiguracji prędkości ich pobierania z serwera zarządzającego.
- 1.8. 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.

6. Moduł centralnego zarządzania

- 1.1. Centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem z pojedynczej konsoli.
- 1.2. Centralna aktualizacja ochrony antywirusowej, zapory ogniowej i systemu wykrywania włamań przez administratora sieci.
- 1.3. Produkt ma wykrywać i raportować nieautoryzowane zmiany w konfiguracji produktu na stacji roboczej. Ma istnieć możliwość blokowania takich zmian.
- 1.4. 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.
- 1.5. Możliwość definiowania wielu niezależnych organizacji na jednym serwerze zarządzającym – informacje dostarczone do serwera zarządzającego nie będą dostępne pomiędzy organizacjami.
- 1.6. Integracja z Microsoft ActiveDirectory w celu importu użytkowników, listy maszyn, struktury jednostek organizacyjnych.
- 1.7. Konta administracyjne mają być tworzone na poziomie serwerów zarządzających i na poziomie organizacji definiowanych na serwerze.
- 1.8. Uprawnienia administratorów mają być ustawiane niezależnie dla każdego kontenera wewnątrz organizacji.
- 1.9. Możliwość utworzenia administratorów z uprawnieniami tylko do odczytu.
- 1.10. Konfiguracja agentów ma mieć strukturę drzewa, z mechanizmami dziedziczenia.
- 1.11. Uwierzytelnianie administratorów ma się odbywać w oparciu o wewnętrzną bazę danych lub z użyciem Microsoft ActiveDirectory. Produkt ma mieć możliwość

wykorzystania wielo-elementowego uwierzytelniania (np. z wykorzystaniem tokenów, certyfikatów itp.).

- 1.12. Dostęp do interfejsu produktu i listy funkcji dostępnych dla użytkownika ma być konfigurowany z poziomu centralnej konsoli zarządzającej.
- 1.13. Konfiguracja aktywna na stacji ma rozróżniać lokalizację agenta i według tego kryterium określać stosowany zestaw reguł/polityk dla agenta.
- 1.14. 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.
- 1.15. Opis lokalizacji powinien zawierać możliwość tworzenia połączeń logicznych „I” oraz „LUB” na powyżej wymienionych elementach.
- 1.16. Paczki instalacyjne produktu mają pozwalać na dodanie własnej konfiguracji.
- 1.17. Pełna funkcjonalność ma być zawarta w jednym pliku instalacyjnym.
- 1.18. Nowe wersje oprogramowania mają być automatycznie dystrybuowane na stacje robocze w postaci różnicy między aktualnie zainstalowaną wersją na kliencie a nową wersją oprogramowania.
- 1.19. Produkt ma automatycznie wykrywać wszystkie urządzenia przyłączone do sieci komputerowej.
- 1.20. Produkt ma zapewniać graficzne raportowanie.
- 1.21. Wbudowane raporty mają pokazywać:
 - stan dystrybucji sygnatur antywirusowych oraz IDS/IPS,
 - wersje zainstalowanych klientów,
 - inwentaryzacje stacji roboczych,
 - wykrytych wirusów, zdarzeń sieciowych, integralności komputerów.
- 1.22. Moduł raportowania ma pokazywać stan wykonywanych poleceń na komputerach.
- 1.23. Możliwość zaplanowanego tworzenia raportów i przesyłania ich do danych kont pocztowych.
- 1.24. Możliwość zdefiniowania alertów administracyjnych zawierających zdarzenia:
 - błędnej autoryzacji do systemu zarządzania,
 - dostępności nowego oprogramowania,
 - pojawienia się nowego komputera,
 - zdarzeń powiązanych z infekcjami wirusów,
 - stanu serwerów zarządzających.
- 1.25. Pełna polska wersja językowa oprogramowania dla systemu zarządzania i stacji klienckich wraz z dokumentacją.

7. Dystrybucja oprogramowania – dodatkowa funkcjonalność

- 1.1. Paczka instalacyjna agenta do zarządzania instalowana na komputerze musi być nie większa niż 20MB.
- 1.2. Agent musi mieć możliwość określenia z jaką przepustowością ma pobierać paczki instalacyjne (musi być też możliwość zdefiniowania, że ograniczenie pasma obowiązuje, jeżeli pasmo jest niższe niż określone).

- 1.3. Musi istnieć możliwość przekształcenia dowolnego agenta w taki sposób by lokalnie mógł dostarczać paczki instalacyjne dla danej grupy agentów – agenci sami wybiorą sobie dla nich najbliższe repozytorium paczek instalacyjnych.
- 1.4. Musi istnieć możliwość zdefiniowania z jaką przepustowością agent przekształcony w lokalne repozytorium ma pobierać paczki instalacyjne – konfiguracja ta ma być niezależna od konfiguracji pozostałych agentów.
- 1.5. Musi istnieć możliwość dowolnego grupowania agentów oraz możliwość importu skonfigurowanych grup z Active Directory.
- 1.6. Agent musi zupełnie niezależnie mieć możliwość naprawy instalacji oprogramowania, dostarczenia nowych definicji wirusów, dokonanie audytu wykorzystywanego oprogramowania antywirusowego (w szczególności wykorzystywanej wersji oprogramowania).
- 1.7. Agent musi mieć możliwość wykonania prostych komend na komputerze opartych o języki skryptowe.

8. Platforma

- 1.1. Oprogramownie musi działać na systemach Windows 2000 Professional i Server, Windows XP 32/64-bit, Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 2003 32/64-bit, Windows 2008 32/64-bit.
- 1.2. Komponenty rozwiązania takie jak: firewall, zapobieganie włamaniom i kontrola integralności komputera muszą działać na wszystkich powyższych platformach 32/64-bitowych.
- 1.3. Serwer zarządzający musi działać na systemach Windows 2003 32/64-bit, Windows 2008 32/64-bit.

9. Dodatkowa ochrona stacji roboczych - wsparcie dla wersji 32/64 bit. -Windows XP/Vista/7

- 1.1. Oprogramowanie dedykowane do backupu i odtwarzania systemów operacyjnych Windows (desktopy, laptopy).
- 1.2. Musi potrafić odtwarzać cały system operacyjny po awarii w ciągu kilku minut, w sposób automatyczny.
- 1.3. Musi potrafić odtwarzać System Windows nawet na sprzęcie innym niż był wykonywany backup.
- 1.4. Musi umożliwiać konwersję do maszyny wirtualnej (VMware Workstation 5.x/6.x, Vmware ESX/ESXi 3.5/4.0, Microsoft Hyper-V 1.0 oraz Server 2008 R2, Citrix XenServer 4.x oraz 5.x).
- 1.5. Musi umożliwiać prostą konwersję z maszyny wirtualnej na fizyczną.
- 1.6. Musi posiadać centralną konsolę do zarządzania środowiskiem.
- 1.7. Możliwość backupu i odtwarzania nie tylko całych dysków ale i pojedynczych plików czy katalogów.
- 1.8. Możliwość integracji z systemami antywirusowymi umożliwiające automatyczne uruchomienie backupu w momencie zidentyfikowania zagrożenia.
- 1.9. Proces odtwarzania systemu musi być oparty na w pełni automatycznym procesie bez konieczności manualnego uaktualniania sterowników sprzętu nawet jeśli jest to inny serwer niż źródłowy.

- 1.10. Dane backupowe mogą być zapisywane na dyskach wymiennych, udziałach sieciowych czy serwerze FTP.
- 1.11. Możliwość zebrania (backupu) całego serwera przed rozpoczęciem cyklu startu systemu („Cold Image Technology”), bez konieczności instalowania oprogramowania na komputerze.
- 1.12. Możliwość integracji z Google Desktop dla sprawnego wyszukiwania plików i folderów poprzez interfejs webowy.
- 1.13. Możliwość balansowania obciążenia procesorów w czasie pracy oprogramowania, dla minimalizacji wpływu na zwykłą pracę serwera czy stacji roboczej.
- 1.14. Możliwość konfigurowania nie tylko backupów pełnych ale i przyrostowych celem zmniejszenia ilości danych gromadzonych i czasu trwania procesu.
- 1.15. Możliwość definiowania zdarzeń które wymuszają automatyczne wykonywanie backupu np. instalacja aplikacji, zalogowanie czy wylogowanie użytkownika.
- 1.16. Wsparcie dla różnych nośników do przechowywania danych: NAS, SAN, USB driver, FireWire driver, CD, DVD.
- 1.17. Musi posiadać funkcję etykietowania dysków USB tak by nawet po zmianie litery dysku backup został wykonany automatycznie.
- 1.18. Możliwość ograniczenia pasma do przesyłu zbackupowanych danych.
- 1.19. Możliwość dodawania poleceń przed i po zakończeniu zadania backupowego.
- 1.20. Możliwość wysyłania komunikatów poprzez protokół SNMP czy SMTP.
- 1.21. Export danych raportowych do csv, html, xml.
- 1.22. Możliwość konfigurowania uprawnień administracyjnych.
- 1.23. Możliwość tworzenia dodatkowej kopii danych i transfer ich poprzez protokół FTP do innej lokalizacji.
- 1.24. Możliwość dostosowywania dysku startowego poprzez możliwość aktualizacji potrzebnych sterowników.

10. Dodatkowa ochrona serwerów - wsparcie dla wersji 32/64 bit. -Windows Server 2003/2008.

- 1.1. Oprogramowanie dedykowane do backupu i odtwarzania systemów operacyjnych Windows (serwery).
- 1.2. Musi potrafić odtwarzać cały system operacyjny po awarii w ciągu kilku minut, w sposób automatyczny.
- 1.3. Musi potrafić odtwarzać System Windows nawet na sprzęcie innym niż był wykonywany backup.
- 1.4. Musi umożliwiać konwersję do maszyny wirtualnej (VMware Workstation 5.x/6.x, Vmware ESX/ESXi 3.5/4.0, Microsoft Hyper-V 1.0 oraz Server 2008 R2, Citrix XenServer 4.x oraz 5.x).
- 1.5. Musi umożliwiać prostą konwersję z maszyny wirtualnej na fizyczną.
- 1.6. Musi posiadać centralną konsolę do zarządzania środowiskiem.
- 1.7. Dla backupu MS Exchange i Sharepoint możliwość odtwarzania pojedynczych maili czy dokumentów.
- 1.8. Możliwość backupu i odtwarzania nie tylko całych dysków ale i pojedynczych plików czy katalogów.
- 1.9. Możliwość integracji z systemami antywirusowymi umożliwiające automatyczne uruchomienie backupu w momencie zidentyfikowania zagrożenia.

- 1.10. Proces odtwarzania systemu musi być oparty na w pełni automatycznym procesie bez konieczności manualnego uaktualniania sterowników sprzętu nawet jeśli jest to inny serwer niż źródłowy.
- 1.11. Dane backupowe mogą być zapisywane na dyskach wymiennych, udziałach sieciowych czy serwerze FTP.
- 1.12. Możliwość zebrania (backupu) całego serwera przed rozpoczęciem cyklu startu systemu („Cold Image Technology”), bez konieczności instalowania oprogramowania na serwerze.
- 1.13. Możliwość balansowania obciążenia procesorów w czasie pracy oprogramowania, dla minimalizacji wpływu na zwykłą pracę serwera czy stacji roboczej.
- 1.14. Możliwość konfigurowania nie tylko backupów pełnych ale i przyrostowych celem zmniejszenia ilości danych gromadzonych i czasu trwania procesu.
- 1.15. Możliwość definiowania zdarzeń które wymuszają automatyczne wykonywanie backupu np. instalacja aplikacji, zalogowanie czy wylogowanie użytkownika.
- 1.16. Wsparcie dla różnych nośników do przechowywania danych: NAS, SAN, USB driver, FireWire driver, CD, DVD.
- 1.17. Musi posiadać funkcję etykietowania dysków USB tak by nawet po zmianie litery dysku backup został wykonany automatycznie.
- 1.18. Możliwość ograniczenia pasma do przesyłu zbackupowanych danych.
- 1.19. Integracja z Microsoft VSS celem backupu danych bazodanowych bez potrzeby ich zatrzymywania.
- 1.20. Możliwość dodawania poleceń przed i po zakończeniu zadania backupowego.
- 1.21. Wsparcie dla backupu kontrolera domeny (Microsoft Active Directory).
- 1.22. Możliwość wysyłania komunikatów poprzez protokół SNMP czy SMTP.
- 1.23. Export danych raportowych do csv, html, xml.
- 1.24. Możliwość konfigurowania uprawnień administracyjnych.
- 1.25. Możliwość tworzenia dodatkowej kopii danych i transfer ich poprzez protokół FTP do innej lokalizacji.
- 1.26. Możliwość dostosowywania dysku startowego poprzez możliwość aktualizacji potrzebnych sterowników.

II Ochrona serwerów pocztowych

1. Ochrona bramy pocztowej

- 1.1. Obsługa dedykowanego urządzenia lub środowiska wirtualne VMware.
- 1.2. Integracja z LDAP: Active Directory, MS Exchange 5.5, Lotus Domino LDAP Server 6.5/7.0/8.x.
- 1.3. Zintegrowane rozwiązanie antywirusowe, antyspamowe i filtrowania treści.
- 1.4. Praca jako bramka pocztowa.
- 1.5. Blokowanie spamu w oparciu o lokalne polityki, silnik skanujący i bazy. Poczta nie jest przekierowywana na serwer usługodawcy.
- 1.6. Rozwiązanie antyspamowe ma mieć skuteczność nie mniejszą niż 98%. Równocześnie rozwiązanie ma charakteryzować się współczynnikiem fałszywych alarmów na poziomie 1 na milion, potwierdzonym przez niezależne testy.
- 1.7. Do wykrywania spamu, system ma wykorzystywać bazy o numerach IP lub nazwach domen wykorzystywanych przez spamerów.

- 1.8. System ma zapewnić routing wiadomości pocztowych w oparciu o domenę i adres odbiorcy.
- 1.9. System ma mieć możliwość zmiany domeny i nazwy użytkownika w wiadomości przychodzącej i wychodzącej dla odbiorcy i nadawcy odpowiednio dla ruchu przychodzącego i wychodzącego.
- 1.10. System ma umożliwiać tworzenie aliasów dla grup użytkowników.
- 1.11. System ma zapewnić dopisywanie domyślnej nazwy domeny dla nadawcy wiadomości.
- 1.12. System ma zapewnić ochronę przed skanowaniem serwera pocztowego w poszukiwaniu istniejących (prawidłowych) adresów pocztowych.
- 1.13. Usuwanie nagłówków Received z wysyłanych wiadomości.
- 1.14. Wiadomości z systemów próbujących atakować spamem serwer pocztowy, mają być automatycznie odrzucane przez określony czas jeśli zostanie przekroczona wartość graniczna (ilość wiadomości zaklasyfikowanych jako spam z jednego IP w danym przedziale czasu).
- 1.15. Wiadomości z systemów próbujących atakować wirusami serwer pocztowy, mają być automatycznie odrzucane przez określony czas jeśli zostanie przekroczona wartość graniczna (ilość wiadomości zaklasyfikowanych jako wirusy z jednego IP w danym przedziale czasu).
- 1.16. Połączenia z systemów próbujących atakować spamem serwer pocztowy, mają być automatycznie odrzucane przez określony czas jeśli zostanie przekroczona wartość graniczna (ilość wiadomości zaklasyfikowanych jako spam z jednego IP w danym przedziale czasu).
- 1.17. Administrator ma mieć możliwość definiowania domen i adresów pocztowych, z którymi wymiana wiadomości będzie się zawsze odbywać.
- 1.18. Administrator ma mieć możliwość definiowania domen i adresów pocztowych, z którymi wymiana wiadomości będzie zawsze blokowana.
- 1.19. Niezależnie konfigurowane polityki dla wiadomości przychodzących i wychodzących.
- 1.20. Funkcja ograniczająca dostępne pasmo dla maszyn/domen przesyłających spam, ale nie blokująca w całości komunikacji z tymi maszynami/domenami.
- 1.21. Aktualizacje sygnatur spamu nie rzadziej niż co 1 min.
- 1.22. Aktualizacje sygnatur antywirusowych nie rzadziej niż co 30-60 minut.
- 1.23. Rozwiązanie antywirusowe ma skanować skompresowane załączniki do 10 poziomów zagnieżdżeń w głąb i ma być odporna na złośliwie spreparowane załączniki („załączniki bomby”).
- 1.24. Wiadomości z wirusami typu mass-mailer mają być w całości odrzucane, bez podejmowania dodatkowych akcji takich jak np. powiadomienie.
- 1.25. Wykrywanie fałszywych URL-i w wiadomościach.
- 1.26. Wykorzystanie technologii znakowania załączników dla odróżnienia ich treści.
- 1.27. Wykorzystanie technologii analizy html mających na celu przeciwdziałanie metodom utrudniającym analizę treści wiadomości (np.: losowo generowane ciągi, nieprawidłowe kody formatujące).
- 1.28. Detekcja języka w którym została napisana wiadomość i możliwość użycia tej informacji jako kryterium przy przetwarzaniu wiadomości.
- 1.29. Kontrola treści w oparciu o słowa kluczowe lub słowniki definiowana przez administratora, w tym sprawdzanie zawartości skompresowanych archiwów.
- 1.30. Możliwość dodawania do wysyłanych wiadomości zdefiniowanego tekstu.

- 1.31. Nakładanie polityk na załączniki w oparciu o ich rozmiar, typ MIME, nazwa pliku lub jego rozszerzenie – w tym identyfikację prawdziwego rozszerzenia pliku.
- 1.32. Wiadomości sklasyfikowane jako spam można:
 - Usunąć,
 - Dodać nagłówek wiadomości,
 - Zmodyfikować – dodać informację dla odbiorcy,
 - Zarchiwizować,
 - BCC – wysłać blind carbon copy na inny adres pocztowy,
 - Bounce – odpowiedzieć nadawcy wiadomością z modyfikowalnym NDR,
 - Wyczyścić jeśli wiadomość zawierała wirusa,
 - Dostarczyć bez modyfikacji,
 - Przekierowywać na inny adres pocztowy,
 - Zmodyfikować temat wiadomości,
 - Wrzucić wiadomość do centralnej kwarantanny,
 - Przesłać powiadomienie na wybrany adres,
 - Usunąć załącznik z wiadomości.
- 1.33. Możliwość wysłania wiadomości spam nie wykrytych przez rozwiązanie do producenta, w celu ich analizy.
- 1.34. Rozróżnienie kategorii wiadomości na:
 - Normalne wiadomości bez spamu i wirusów,
 - Spam,
 - Podejrzane o spam,
 - Wirusy masowe,
 - Wiadomości zawierające wirusy,
 - Wiadomości których nie można przeskanować,
 - Wiadomości od blokowanych nadawców,
 - Wiadomości zablokowane na podstawie filtrów przygotowanych przez administratora.
- 1.35. Wsparcie dla Transport Layer Security (TLS) – definiowane per domena lub polityka, Sender Policy Framework (SPF), Sender ID.
- 1.36. Import bazy użytkowników poprzez LDA.
- 1.37. Administrator ma mieć możliwość ingerencji w zaufaniu rozwiązania.
- 1.38. Rozwiązanie ma posiadać serwer kwarantanny, Serwer ma być dostępny dla poszczególnych użytkowników końcowych. Serwer ma przysyłać okresowe powiadomienia o zawartości kwarantanny. Powiadomienia mają mieć wbudowane mechanizmy do zarządzania zawartością kwarantanny (przesłanie dalej, podgląd, zalogowanie do kwarantanny).
- 1.39. Na serwer kwarantanny można nałożyć ograniczenia dla poszczególnych użytkowników jak i całego serwera wg ilości przechowywanych wiadomości, ilości zajętego miejsca.
- 1.40. Użytkownik końcowy rozwiązania ma mieć możliwość definiowania własnych list blokowanych i przepuszczanych nadawców wiadomości, ingerencje w zachowanie systemu detekcji języka i możliwość wysłania do producenta systemu źle sklasyfikowanych wiadomości.
- 1.41. Komunikacja pobierania uaktualnień ma być szyfrowana. Komunikacja w celu zarządzania systemem ma być szyfrowana.

- 1.42. Rozwiązanie ma być centralnie zarządzane z wbudowanymi mechanizmami raportowania. Jedna konsola ma umożliwić zarządzania kilkoma współpracującymi urządzeniami. Wykonywane raporty mają uwzględniać dane zebrane ze wszystkich współpracujących urządzeń.
- 1.43. System ma posiadać min 55 wbudowanych raportów. Wykonanie raportów można zaplanować w dzienniku. Gotowe raporty można przesłać do skrzynki pocztowej wyznaczonych odbiorców.
- 1.44. System ma umożliwiać tworzenie wielu kont administracyjnych z różnymi poziomami uprawnień, w tym możliwość zdefiniowania użytkowników mających dostęp do różnych kwarantann.
- 1.45. System ma umożliwiać definiowanie poziomu logowania o swojej aktywności.
- 1.46. System ma powiadamiać wybranych administratorów o nieprawidłowej pracy komponentów.
- 1.47. System ma umożliwiać wykonywanie zaplanowanych kopii bezpieczeństwa konfiguracji i baz kwarantanny oraz możliwość odtworzenia konfiguracji z tak wykonanej kopii.
- 1.48. Ograniczony zestaw poleceń dostępny z konsoli systemu operacyjnego.
- 1.49. System ma umożliwiać graficzne śledzenie wiadomości, w tym informacje co stało się z wiadomością.
- 1.50. System ma posiadać wewnętrzną bazę reputacji, śledzącą adresy IP serwerów pocztowych.
- 1.51. System ma umożliwiać zapytanie o adres IP do wewnętrznej i globalnej bazy reputacji.
- 1.52. System ma umożliwiać stworzenie odpowiednio obsługiwanych kolejek z punktu widzenia reputacji danego adresu IP – ograniczając taki adres do ilości wysyłanych wiadomości, ilości nawiązywanych połączeń w określonym czasie.
- 1.53. System ma mieć możliwość zdefiniowania osobnej kwarantanny dla poczty naruszającej reguły zgodności z polityką określającą rodzaj przesyłanych treści.
- 1.54. System musi umożliwiać skorzystania z predefiniowanych polityk i wzorców.
- 1.55. System ma umożliwiać rozpatrywanie incydentów skojarzonych z naruszeniem polityk, w tym definiowanie ważności incydentu.
- 1.56. System ma posiadać ochronę przed atakami wirusów typu Day Zero, oraz zdefiniowaną kwarantannę dla złapanych w ten sposób wirusów z możliwością ustawienia czasu przez który zatrzymane maile mają w niej pozostawać.
- 1.57. System ma dodatkowo posiadać możliwość wysyłania alertów SNMP.
- 1.58. System ma umożliwiać integracje z UPS-em.
- 1.59. System musi wspierać autentykację DomainKeys Identified Mail (DKIM).
- 1.60. System musi wspierać autentykację SMTP.

2. Ochrona serwerów Exchange

- 1.1. Wspierane systemy operacyjne: Windows Server 2003 (32/64 bit) oraz Windows Server 2008 (32/64 bit).
- 1.2. Wspierane wersje Exchange: Exchange Server 2003/2007/2010 w wersji Standard lub Enterprise.
- 1.3. Zintegrowane rozwiązanie antywirusowe i opcjonalnie antyspamowe.
- 1.4. Możliwość zdefiniowania precyzyjnej polityki skanowania poczty elektronicznej.
- 1.5. Możliwość tworzenia własnych raportów i ich automatycznego uruchamiania się.

- 1.6. Zawiera zintegrowane narzędzie raportujące służące do raportowania statystyk związanym ze spamem i antywirusem.
- 1.7. Możliwość tworzenia zaplanowanego skanowania zasobów.
- 1.8. Skanowanie wiadomości przesyłanych przez serwer (routed messages).
- 1.9. Możliwość wyboru pojedynczych skrzynek roboczych i folderów publicznych do skanowania zaplanowanego.
- 1.10. Możliwość ustalenia czasu, w którym zaplanowane skanowanie ma się odbywać (okno czasowe). W przypadku, gdy skanowanie nie zostanie zakończone, następne skanowanie rozpocznie się w miejscu zakończenia poprzedniego.
- 1.11. Aktualizacja definicji wirusów, co 1 godzinę.
- 1.12. Wykorzystanie VS API 2.5.
- 1.13. Wbudowana heurystyka.
- 1.14. Usuwanie załączników o niepożądanym rozszerzeniu, także w archiwach spakowanych.
- 1.15. Blokowanie wysyłania załączników dla grup użytkowników (integracja z Active Directory), dla wiadomości przychodzących czy wychodzących.
- 1.16. Blokowanie wysyłania wiadomości z uwagi na treść dla grup użytkowników (integracja z Active Directory), dla wiadomości przychodzących czy wychodzących.
- 1.17. Monitorowanie pracy systemu AV na serwerze Exchange'a, w celu wykrycia problemów z komunikacją system AV – Exchange.
- 1.18. Konfiguracja przesyłanych powiadomień w zależności od rodzaju wykrytego zagrożenia.
- 1.19. Możliwość usuwania całych wiadomości w przypadku wykrycia wirusa.
- 1.20. Możliwość ciągłego skanowania Information Store w czasie rzeczywistym.
- 1.21. Możliwość korzystania z centralnego serwera kwarantanny.
- 1.22. Powiadamianie administratora o zmasowanym ataku wirusów.
- 1.23. Funkcja usuwania poczty masowej automatycznie (Mass-Mailer Cleanup) eliminuje nie tylko załączniki, lecz całe wiadomości zainfekowane przez robaki rozsyłające się masowo za pomocą poczty elektronicznej.
- 1.24. Niestandardowe reguły filtrowania.
- 1.25. Filtrowanie oparte na regułach zapobiega przedostawaniu się do sieci niepożądanych treści, a także wydostawaniu się z niej poufnych informacji.
- 1.26. Centralne zarządzanie za pomocą jednej konsoli obsługującej wiele serwerów, umożliwiające jednoczesną aktualizację ustawień wszystkich serwerów Microsoft® Exchange w całym przedsiębiorstwie.
- 1.27. Zawiera narzędzie do zwalczania nowych „nieznanych” wirusów.
- 1.28. Możliwość definiowania reguł dla plików zaszyfrowanych.
- 1.29. Możliwość eksportowania i importowania ustawień konfiguracyjnych.
- 1.30. System ma umożliwiać identyfikację prawdziwego typu pliku niezależnie od jego rozszerzenia.
- 1.31. Zintegrowane rozwiązanie antywirusowe i antyspamowe, jedna konsola zarządzająca.
- 1.32. Blokowanie spamu w oparciu o lokalne polityki, silnik skanujący i bazy. Poczta nie jest przekierowana na serwer usługodawcy.
- 1.33. Definiowalne reguły filtrowania oraz funkcje obsługi czarnych list i białych list w czasie rzeczywistym.

- 1.34. Rozwiązanie antyspamowe ma mieć skuteczność nie mniejszą niż 97%.Równocześnie rozwiązanie ma charakteryzować się współczynnikiem fałszywych alarmów na poziomie 1 na milion, potwierdzonym przez niezależne testy.
- 1.35. Do wykrywania spamu, system ma wykorzystywać bazy o numerach IP lub nazwach domen wykorzystywanych przez spamerów.
- 1.36. Aktualizacje sygnatur spamu nie rzadziej, niż co 10 min.
- 1.37. Możliwość definiowania reguł dotyczących wiadomości podejrzanych o spam i uznanych za spam.
- 1.38. Automatyczny sposób uaktualniania definicji antywirusów i antyspamu.
- 1.39. integracja z funkcjami określania poziomu wiarygodności poczty przychodzącej (Spam Confidence Level) oraz inteligentnego filtrowania wiadomości (Intelligent Message Filter) firmy Microsoft.
- 1.40. System ma posiadać wewnętrzną bazę reputacji, śledzącą adresy IP serwerów pocztowych.

III Wsparcie techniczne

Wsparcie techniczne polegające na pomocy w przypadkach awarii bądź błędnego działania zakupionego oprogramowania antywirusowego. Preferowanymi formami kontaktu Zamawiającego z Wykonawcą są: poczta elektroniczna oraz kontakt telefoniczny. Numery telefonów oraz adresy email, wsparcia technicznego, Wykonawca poda w umowie.