Wymagania dotyczące system ochrony antywirusowej z zaporą ogniową dla stacji roboczych i serwerów.

1. Istotne cechy oprogramowania :

A. Pełne wsparcie dla systemu Windows: 8, 7, Vista, Server 2012, 2008, Linux (tylko klient).

B. Wsparcie dla 64-bitowych wersji systemu Windows: 8, 7, Vista, Server 2012, 2008 Server.

C. Ochrona w sesji RDP na serwerach Windows Server 2012 R2,

D. Ochrona antywirusowa wyżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli

E. Interfejsy programu, pomoce i podręczniki w języku polskim.

F. Pomoc techniczna w języku polskim.

2. Ochrona antywirusowa

A. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

B. Wykrywanie i usuwanie niebezpiecznych programów: adware, spyware, scareware, phishing, hacktools itp.

C. Ochrona przed rootkitami wykrywająca aktywne i nieaktywne rootkity.

D. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

E. Możliwość wykluczenia ze skanowania skanera dostępowego: napędów, katalogów, plików lub procesów.

F. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików na żądanie lub według harmonogramu.

G. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).

H. Skanowanie na żądanie pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.

I. Technologia zapobiegająca powtórnemu skanowaniu sprawdzonych już plików, przy czym maksymalny czas od ostatniego sprawdzenia pliku nie może być dłuższy niż 4 tygodnie, niezależnie od tego czy plik był modyfikowany czy nie.

J. Możliwość określania poziomu obciążenia procesora podczas skanowania na żądanie i według harmonogramu.

K. Możliwość skanowania dysków sieciowych i dysków przenośnych.

L. Rozpoznawanie i skanowanie wszystkich znanych formatów kompresji.

M. Możliwość definiowania listy procesów, plików, folderów i napędów pomijanych przez skaner dostępowy.

N. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji modułu antywirusowego.

O. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.

P. Dodatek do aplikacji MS Outlook umożliwiający podejmowanie działań związanych z ochroną z poziomu programu pocztowego.

Q. Skanowanie i oczyszczanie poczty przychodzącej POP3 w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

R. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.

S. Możliwość definiowania różnych portów dla POP3, SMTP i IMAP na których ma odbywać się skanowanie.

T. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.

U. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.

V. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

W. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe.

X. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.

Y. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e mail.

Z. Możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.

AA. Aktualizacja dostępna z bezpośrednio Internetu lub offline – z pliku pobranego zewnętrznie.

BB. Możliwość samodzielnej aktualizacji sygnatur wirusów ze stacji roboczej (np. komputery mobilne).

CC. Możliwość ukrycia programu na stacji roboczej przed użytkownikiem.

DD. Kontrola zachowania aplikacji do wykrywania podejrzanie zachowujących się aplikacji.

EE. Skanowanie w trybie bezczynności - pełne skanowanie komputera przynajmniej raz na 2 tygodnie uruchamiane i wznawiane automatycznie, podczas gdy nie jest on używany.

3. Zdalne administrowanie ochroną

A. Pełna integracja z Active Directory – import kont komputerów i jednostek organizacyjnych.

B. Opcja automatycznej instalacji oprogramowania klienckiego na wszystkich podłączonych komputerach Active Directory.

C. Zdalna instalacja oprogramowania klienckiego na stacjach roboczych Windows.

D. Do instalacji zdalnej i zarządzania zdalnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy.

E. Możliwość zarządzania ochroną urządzeń mobilnych z poziomu konsoli (przynajmniej aktualizacje, ochronę przeglądarek, skanowania zasobów, synchronizacji raportów)

F. Możliwość kontekstowego zastosowania ustawień danej stacji dla całej grupy.

G. Możliwość eksportu/importu ustawień dla stacji/grupy stacji

H. Możliwość zarządzania dowolną ilością serwerów zarządzających z jednego okna konsoli.

I. Możliwość zarządzania różnymi wersjami licencyjnymi oprogramowania producenta z jednego okna konsoli.

J. Możliwość tworzenia hierarchicznej struktury serwerów zarządzających (serwer główny i serwery podrzędne).

K. Możliwość zainstalowania zapasowego serwera zarządzającego, przejmującego automatycznie funkcje serwera głównego w przypadku awarii lub odłączenia serwera głównego.

L. Możliwość zdalnego zarządzania serwerem centralnego zarządzania przez przeglądarki internetowe (z sieci lokalnej i spoza niej).

M. Szyfrowanie komunikacji między serwerem zarządzającym a klientami.

N. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.

O. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania).

P. Możliwość sprawdzenia z centralnej konsoli zarządzającej zainstalowanych na stacjach/serwerach oprogramowania (tj. nazwa, wersja, producent, data instalacji).

Q. Możliwość stworzenia białej i czarnej listy oprogramowania, i późniejsze filtrowanie w poszukiwaniu stacji je posiadających.

R. Odczyt informacji o zasobach stacji (procesor i jego taktowanie, ilość pamięci RAM i ilość miejsca na dysku

S. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.

T. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.

U. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.

V. Możliwość zmiany konfiguracji na stacjach i serwerach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).

W. Możliwość przeglądania statystyk ochrony antywirusowej w postaci tekstu lub wykresów.

X. Możliwość przesłania komunikatu, który wyświetli się na ekranie wybranej stacji roboczej lub grupie stacji roboczych.

Y. Komunikat można wysłać do wszystkich lub tylko wskazanego użytkownika stacji roboczej.

Z. Możliwość zminimalizowania obciążenia serwera poprzez ograniczenie ilości jednoczesnych procesów synchronizacji, aktualizacji i przesyłania plików do stacji roboczych.

4. Raporty

A. Możliwość utworzenia raportów statusu ochrony sieci.

B. Możliwość wysyłania raportów z określonym interwałem.

C. Możliwość wysłania jednego raportu na różne adresy mailowe lub grupy adresów.

D. Możliwość zdefiniowania różnych typów informacji dotyczących statusu ochrony oraz różnych form ich przedstawienia (tabele, wykresy) w pojedynczym raporcie.

5. Osobista zapora połączeń sieciowych

A. W pełni zdalna instalacja, zdalne zarządzanie wszystkimi funkcjami zapory i zdalna deinstalacja.
B. Zapora działająca domyślnie trybie automatycznego rozpoznawania niegroźnych połączeń i tworzenia reguł bez udziału użytkownika.
C. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
D. Możliwość zdefiniowania osobnych zestawów reguł dla dowolnych grup użytkowników.
E. Wbudowany system IDS.
F. Możliwość pracy w trybie offsite, po odłączeniu od sieci przedsiębiorstwa.
G. Wykrywanie zmian w aplikacjach korzystających z sieci na podstawie sum kontrolnych i monitorowanie o tym zdarzeniu.
H. Możliwość automatycznego skanowania antywirusowego modułów o zmodyfikowanych sumach kontrolnych.
I. Automatyczne wysyłanie powiadomień o zablokowaniu aktywności sieciowej na wskazany adres mailowy.
J. Import/eksport reguł/zestawów reguł zapory na stacji roboczej