Wymagania dotyczące system ochrony anty wirusowej z zaporą ogniową dla stacji roboczych.

Istotne cechy oprogramowania :

1. ochrona antywirusowa stacji roboczych (Windows 7 32-bit i 64-bit Windows Vista 32-bit i 64-bit)
2. ochrona antywirusowa wyżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli
3. możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach.
4. polski interfejs użytkownika i dokumentacja do oprogramowania na stację roboczą

Wymagania dotyczące technologii:

1. ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy
2. oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan"
3. aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie plików i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu,
4. możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta,
5. aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie
6. brak konieczności restartu komputerów po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów
7. heurystyczna technologia do wykrywania nowych, nieznanych wirusów,
8. wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit"
9. możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie
10. Mechanizm centralnego zarządzania folderami kwarantanny znajdującymi się na stacjach klienckich.
11. mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona,
12. mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji),
13. obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym co najmniej : ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2

14. automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa,
15. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji,
16. automatyczne uruchamianie procedur naprawczych,
17. uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione,
18. gwarancja na dostarczenie szczepionki na nowego wirusa w czasie krótszym niż 48 godzin,
19. średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365),
20. automatyczne powiadomienie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem stacja robocza jest odpowiednio zabezpieczona
21. skanowanie przez program na komputerze klienckim przychodzącej i wychodzącej poczty elektronicznej bez konieczności instalowania dodatkowych programów/modułów. W programach pocztowych nie modyfikowane są ustawienia konta, tj. serwera POP3, SMTP i IMAP. Obsługuje m.in. MS Outlook Express, MS Outlook, Mozilla, Eudora, Netscape Mail,
22. skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu HTTP
23. automatyczna kwarantanna blokująca ruch przychodzący i wychodzący, włączająca się w momencie gdy stacja robocza posiada stare sygnatury antywirusowe
24. wsparcie dla technologii Cisco Network Admission Control (NAC)
25. ochrona przeglądarki internetowej, w tym : blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX i pobieranych plików
26. Ochrona podczas przeglądania sieci Internet przy pomocy – integracja z przeglądarką internetową Internet Explorer 6 oraz Mozilla 2 (lub wyższe wersje)
27. Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębną plik wykonywalny dostarczony przez producenta.
28. Możliwość pobierania aktualizacji przez klientów między sobą – tzw. „Neighborcast" pozwalające na odciążenie łącza do sieci WAN,
29. ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji,
30. kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną
31. osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych

Wymagania dotyczące systemy zarządzania centralnego:

1. Konsola zarządzania umożliwia eksport pakietu instalacyjnego dla klienta w formacie Microsoft Installer (MSI) i JAR lub też bezpośrednią instalację zdalną nienadzorowaną
2. narzędzie instalacyjne musi sprawdzać istnienie poprzednich wersji oprogramowania. W przypadku znalezienia poprzedniej wersji instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie z klienta lub serwera i instalować nowe wersję,
3. pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem),
4. komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi
5. pełne centralne zarządzanie dla Windows Server 2008, Windows Vista, Windows 7,
6. scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta,
7. administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa
8. centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy,
9. możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów)
10. tworzenie grup , zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach,
11. możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych i w celu uniemożliwienia ich modyfikacji przez użytkowników,
12. możliwość wyłączenia blokady zmiany ustawień dla użytkownika z prawami administratora
13. serwer zarządzający związany z konsolą zarządzającą musi mieć funkcję przesyłania aktualizacji do klientów z możliwością ustawienia harmonogramu lub częstotliwości aktualizacji,
14. możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający,
15. możliwość instalacji i konfiguracji wewnętrznego serwera aktualizacji, łączącego się z serwerem aktualizacji producenta i aktualizacja serwerów, serwera zarządzającego oraz stacji roboczych z wewnętrznego serwera aktualizacji,
16. możliwość ustalenia dodatkowego harmonogramu pobierania przez serwery plików i stacje robocze aktualizacji z serwera producenta,
17. funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania,
18. dane powinny być przesyłane do serwera zarządzania podczas kolejnego połączenia,

19. możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich,
20. umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe,
21. automatyczne wykrywanie i usuwanie oprogramowanie innych wiodących producentów systemów antywirusowych (min. 3 inne) podczas instalacji,
22. automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej niż co 7 dni (zalecane codzienne aktualizacje),
23. automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe,
24. możliwość eksportu raportów z pracy systemu do pliku MS Excel
25. możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich,
26. możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”,
27. możliwość lokalnego zarządzania wszystkimi ustawieniami programu klienta,
28. program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa,
29. program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe,
30. program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy),
31. program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów,
32. zarządzanie zdarzeniami i raportowanie – natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta elektroniczna, powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania.