Wymagania dotyczące systemu ochrony antywirusowej z zaporą ogniową dla stacji roboczych.
Istotne cechy oprogramowania :

1. Ochrona antywirusowa stacji roboczych :
- Microsoft Windows XP with SP3 (32-bit)
- Microsoft Windows Vista (32-bit i 64-bit)
- Microsoft Windows Vista SP1 lub nowszy (32-bit i 64-bit)
- Microsoft Windows 7 (32-bit i 64-bit)
- Microsoft Windows 7 SP1 lub nowszy (32-bit i 64-bit)
- Microsoft Windows 8 (32-bit i 64-bit)
2. Ochrona antywirusowa wyżej wymienionego systemu monitorowana i zarządzana z portalu zarządzającego dostępnego on-line przez przeglądarkę internetową.
3. Możliwość podłączenia stacji do zdalnego portalu zarządzającego niezależnie na kilku wybranych stacjach.
4. Polski interfejs użytkownika i dokumentacja do oprogramowania na stację roboczą.
5. Sprzedający musi posiadać niezależny od klienta końcowego dostęp do komputerów klienta końcowego podpiętych do portalu zarządzającego

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. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.
3. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”.
4. Skanowanie poczty e-mail pod kątem niepożądanych wiadomości (ochrona anty-spamowa) ; ochrona przed phishingiem.
5. 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.
6. Możliwość wywołania skanowania na żądanie z poziomu portalu zarządzającego dla pojedynczego lub wielu komputerów lub lokalnie przez określonego klienta.
7. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
8. Brak konieczności restartu komputerów po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
9. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
10. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”, „rootkit”.
11. Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger”, „dialer”, „trojan” w kwarantannie.
12. 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.
13. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.
14. 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).
15. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym co najmniej : ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.

16. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.
17. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.
18. Automatyczne uruchamianie procedur naprawczych.
19. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
20. Gwarancja na dostarczenie szczepionki na nowego wirusa w czasie krótszym niż 48 godzin.
21. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).
22. 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.
23. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.
24. Automatyczna kwarantanna blokująca ruch przychodzący i wychodzący, włączająca się w momencie gdy stacja robocza posiada stare sygnatury antywirusowe.
25. Ochrona podczas przeglądania sieci Internet przy pomocy – integracja z przeglądarką internetową Internet Explorer 6 oraz Mozilla 2 (lub wyższe wersje).
26. Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębny plik wykonywalny dostarczony przez producenta.
27. Możliwość pobierania aktualizacji przez klientów między sobą – tzw. „Neighborcast" pozwalające na odciążenie łącza do sieci WAN.
28. Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji.
29. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.
30. Osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.
31. Brak konieczności restartu komputera po zainstalowaniu aplikacji w środowisku Windows Vista/7.
32. Moduł służący aktualizacji oprogramowania firm trzecich wraz z aktualizacjami systemu Windows.

Wymagania dotyczące systemu zarządzania centralnego:

1. Portal zarządzający wraz z edytorem profilów bezpieczeństwa dostępny w języku polskim,
2. Portal zarządzający umożliwia pobranie plików instalacyjnych stacji roboczych oraz stacji serwerowych oraz pobranie narzędzia instalacji zdalnej,
3. 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 nową wersję,
4. Administracja, konfiguracja profilów bezpieczeństwa i monitorowanie stacji roboczych i serwerów plików za pomocą portalu zarządzającego,
5. Komunikacja pomiędzy portalem zarządzającym, a stacjami roboczymi podpisywana jest po instalacji oprogramowania oraz bazuje na podstawie wpisywanego podczas procesu instalacji klucza instalacyjnego,

6. Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, portal zarządzający pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta,
7. Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów,
8. Portal zarządzający musi umożliwiać usuwanie klientów ze swoich grup z całkowitym zachowaniem ustawień oraz przypisanych profili bezpieczeństwa,
9. Tworzenie grup , zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach,
10. Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych i w celu uniemożliwienia ich modyfikacji przez użytkowników,
11. Portal zarządzający musi mieć możliwość wysłania żądania aktualizacji stanu stacji roboczej w celu odświeżenia informacji w portalu zarządzającym,
12. Funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania,
13. Dane powinny być przesyłane do portalu zarządzającego podczas kolejnego połączenia,
14. Automatyczne wykrywanie i usuwanie oprogramowanie innych wiodących producentów systemów antywirusowych (min. 3 inne) podczas instalacji,
15. Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej niż co 7 dni (zalecane codzienne aktualizacje),
16. Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe,
17. Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”,
18. Portal zarządzający musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa,
19. Portal zarządzający musi pozwalać na określenie wykluczonych obszarów ze skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe,
20. Program musi pozwalać na określenie typów skanowanych plików