Załącznik nr 1 do zapytania ofertowego OR 271.1.1.2011

Wymagania dotyczące oprogramowania antywirusowego dla systemów Windows 2000/XP/Vista/7 :

1. ochrona stacji roboczych (Windows 2000, Windows XP, Windows Vista 32 i Vista 64 bity/7),
2. ochrona całego systemu monitorowana i zarządzana z pojedynczej konsoli, zarówno po stronie administratora jak i użytkownika końcowego,
3. możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach
4. polski interfejs użytkownika,
5. ochrona antywirusowa realizowana na trzech poziomach, tj.: monitora kontrolującego system w tle, modułu skanującego nośniki danych i monitora poczty elektronicznej,
6. co najmniej trzy różne silniki antywirusowe, każdy z dedykowanymi bazami sygnatur, funkcjonujące jednocześnie i skanujące wszystkie dane,
7. oddzielny, zintegrowany silnik antyrootkitowy,
8. co najmniej dwa dedykowane silniki antyspyware,
9. 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,
10. możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta,
11. aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie operacyjnym,
12. brak konieczności restartu komputerów po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów,
13. heurystyczna technologia do wykrywania nowych, nieznanych wirusów,
14. wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu "spyware", "adware", "keylogger", "dialer", "trojan",
15. 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,
16. mikrodefinicje wirusów przyrostowe (inkrementalne)- pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stacje kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji),
17. obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym co najmniej : ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2,
18. automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa,
19. automatyczne uruchamianie procedur naprawczych,
20. oprogramowanie zapewnia w procesie skanowania ręcznego i automatycznego przeskanowanie dowolnego celu pod względem wirusów, spyware, rootkitów, riskware,
21. program posiada kwarantannę wirusów, spyware oraz riskware,
22. program z Menu Start pozwala stworzyć plik diagnostyczny do analizy problemów,
23. program pozwala z interfejsu graficznego użytkownika wysłać próbkę wirusa bezpośrednio do laboratorium antywirusowego producenta,

24. uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione,
25. program posiada narzędzie ręcznej aktualizacji stacji roboczych we wszystkie sygnatury dla poszczególnych silników skanujących,
26. gwarancja na dostarczenie szczepionki na nowego wirusa w czasie krótszym niż 48 godzin,
27. średni czas reakcji producenta na nowego wirusa wynosi poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365),
28. automatyczne powiadomienie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem, czy stacja robocza jest odpowiednio zabezpieczona,
29. 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; obsługa i wsparcie techniczne dla m. in. MS Outlook, Express, MS Outlook, Mozilla, Eudora, Netscape Mail,
30. skanowanie przez program na komputerze klienckim danych pobieranych i wysyłanych danych przy pomocy protokołu HTTP na poziomie WinSocks na wszystkich portach , na których odbywa się komunikacja,
31. automatyczna kwarantanna blokująca ruch przychodzący i wychodzący realizowana na poziomie oferowanego oprogramowania, włączająca się w momencie gdy stacja robocza posiada stare sygnatury antywirusowe,
32. program posiada wsparcie do filtrowania protokołu IPv6,
33. ochrona przeglądarki internetowej, w tym: blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX i pobieranych plików,
34. ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji,
35. kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną,
36. osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych, z możliwością automatycznego ustawiania profilu w zależności od lokalizacji, w której znajduje się stacja robocza,
37. oprogramowanie zapewnia uruchomienie podejrzanej aplikacji w wirtualnym środowisku, w pełni odizolowanym od rzeczywistego systemu operacyjnego; wirtualne środowisko powinno odwzorować sieciową stację Windows z Windows API z pełną emulacją x86,
38. oprogramowanie zapewnia sprawdzanie w czasie rzeczywistym nieznanych aplikacji poprzez zapytania przesyłane poprzez sieć do systemu serwerów producenta
39. możliwość aktualizacji oprogramowania antywirusowego na maszynie ze stacji sąsiadującej w sieci LAN.