Załącznik nr 4 do SIWZ

Szczegółowy opis przedmiotu zamówienia

Poniższe zestawienie zawiera opis parametrów minimalnych (równoważnych), jakie powinien spełniać oferowany sprzęt komputerowy.

1	**Komputer biurowy wraz z oprogramowaniem**		**10szt.**
	Procesor:	w architekturze x86 częstotliwość taktowania procesora 3.2 GHz, pojemność cache L3 min. 4 MB ilość rdzeni 2, 4 wątki	
	Pamięć RAM:	4 GB DDR3-1333,	
	Płyta główna:	Płyta główna umożliwiająca obsługę procesora zaoferowanego przez Wykonawcę,. Obsługa dual Channel DDR3. min 2 sloty pamięci, min. 2 złącza PCI, wbudowana karta sieciowa 10/100/1000, złącza IDE ATA – min. 1 szt., złącza SATA – min. 4 szt., gniazdo COM – min. 1 szt., gniazdo LPT – TAK złącza USB – min. 8 szt. (w tym 4 zewnętrzne) Wymagana ilość portów nie może być uzyskana przez stosowanie przejściówek.	
	Karta graficzna:	Zintegrowana z płytą główną lub jako oddzielny komponent, pamięć min. 256 MB	
	Dysk twardy:	Pojemność min. 500GB, SATA II, prędkość obrotowa min. 7200 obr. / min,	
	Napęd optyczny:	Nagrywarka DVD+/-RW DL, rodzaj interfejsu: SATA, dołączone oprogramowanie do nagrywania płyt	
	Napęd FDD:	TAK, 1,44 MB	
	Obudowa:	Tower Micro-ATX lub ATX, napędy zamontowane w pozycji poziomej, min. 2 porty USB dostępne na przednim panelu ilość kieszeni zewnętrznych 3,5” - min. 2 szt. ilość kieszeni zewnętrznych 5,25” - min. 2 szt.	
	Wyposażenie dodatkowe:	-Czytnik kart MD, MC, MS, MMC, SD, CF; -PenDrive 8GB	
	Zasilacz:	Moc min. 400W, zgodny z normą ATX, wentylator z automatyczną regulacją prędkości obrotowej,	
	Oprogramowanie:	System operacyjny: Windows 7 PL Professjonal, dołączone nośniki do instalacji oprogramowania. Oprogramowanie biurowe: MS Office 2010 PKC PL, dołączone nośniki do instalacji oprogramowania	
	Peryferia:	Klawiatura USB, Mysz optyczna USB, podkładka pod mysz peryferia o kolorystyce zgodnej z kolorystyką jednostki centralnej	
	Gwarancja:	Minimum 24 miesiące w miejscu eksploatacji. Czas reakcji serwisu do końca następnego dnia roboczego.	
	Certyfikaty:	Certyfikat bezpieczeństwa CE	

2	**Monitor LCD**		**10 szt.**
	Przekątna:	17”	
	Rozdzielczość nominalna:	1280 x 1024 piksele	
	Nasycenie kolorów	72% (NTSC)	
	Plamka	0,264mm	
	Rodzaj matrycy	Matowa	
	Współczynnik Kontrastu :	1:50000	
	Jasność:	250 cd / m^2	
	Czas reakcji:	5 ms	
	Kąt widzenia pion:	160 st.	
	Kąt widzenia poziom:	160 st.	
	Wbudowane głośniki:	TAK, stereo	
	Wejścia/Wyjścia	Wejście PC:DVI-D/D-Sub, Wejście PC Audio: 3,5mm Mini-jack	
	Klawisze funkcji	Automatyczna regulacja, regulacja jasności, regulacja głośności	
	Uwagi:	Kolorystyka obudowy zgodna z kolorystyką zaoferowanego komputera osobistego PC	
	Spełniane normy jakościowe:	• EPA Energy Star • TCO-03 • UL • CUL • CB • CE • FCC • CCC • ISO 9241-3,7,8 • BSMI • GOST-R • C-TICK • VCCI • PSB • NOM • J-MOSS • ROHS • WHQL	
	Gwarancja:	Minimum 36 miesięcy	

2	**Program antywirusowy**	**50 szt. licencji/24m-ce**

1. Pełne wsparcie dla systemu Windows NT 4.0 z sp6 /2000/2003/XP/ Vista/Windows 7.
2. Wsparcie dla Windows Security Center (Windows XP SP2).
3. Wsparcie dla 32- i 64-bitwej wersji systemu Windows.
4. Wersja programu dla stacji roboczych Windows dostępna zarówno języku polskim jak i angielskim.
5. Pomoc w programie (help) w języku polskim.
6. Dokumentacja do programu dostępna w języku polskim.
7. Skuteczność programu potwierdzona nagrodami VB100 i co najmniej dwie inne niezależne organizacje np. ICSA labs lub Check Mark.

Ochrona antywirusowa i antyspyware

8. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
9. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
10. Wbudowana technologia do ochrony przed rootkitami.
11. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
12. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
13. System powinien oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
14. 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).
15. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
16. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
17. Możliwość skanowania dysków sieciowych i dysków przenośnych.
18. Skanowanie plików spakowanych i skompresowanych.
19. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).
20. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
21. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
22. 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.
23. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).
24. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird i Windows Live Mail
25. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na

stacji roboczej (niezależnie od konkretnego klienta pocztowego).

26. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
27. Możliwość definiowania różnych portów dla POP3, na których ma odbywać się skanowanie.
28. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
29. Możliwość skanowania na żądanie lub według harmonogramu baz Outlook Express-a.
30. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
31. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występujące w nawie strony.
32. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
33. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
34. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
35. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
36. Aktualizacje modułów analizy heurystycznej.
37. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie powinny być wysyłane automatycznie, oraz czy próbki zagrożeń powinny być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
38. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
39. Wysyłanie zagrożeń do laboratorium powinno być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
40. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe.
41. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
42. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.
43. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
44. Interfejs programu powinien oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.
45. Interfejs programu powinien mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb wysokiego kontrastu.
46. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych

protokołów HTTPS i POP3S.

47. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
48. Administrator powinien mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
49. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
50. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.
51. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji powinno być takie samo.
52. Program powinien być w pełni zgodny z technologią CISCO NAC.
53. Program powinien mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
54. Program powinien mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie, powinna także istnieć opcja dezaktywacji tego mechanizmu.
55. Po instalacji programu, użytkownik powinien mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
56. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
57. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien pracować w trybie graficznym.
58. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD oraz portów USB.
59. Funkcja blokowania portów USB powinna umożliwiać administratorowi zdefiniowanie listy portów USB w komputerze, które nie będą blokowane (wyjątki).
60. W programie powinien być wyposażony w funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
61. Funkcja generująca taki log powinna oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
62. Program powinien oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
63. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
64. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej (program antywirusowy z wbudowanym serwerem HTTP).
65. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
66. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).

67. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).
68. Możliwość przypisania 2 profili aktualizacyjnych z różnymi ustawieniami do jednego zadania aktualizacji. Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu.
69. Program wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
70. Praca programu musi być niezauważalna dla użytkownika.
71. Program powinien posiadać dwie wersje interfejsu (standardowy – z ukrytą częścią ustawień oraz zaawansowany – z widocznymi wszystkimi opcjami)
72. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
73. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Konsola zdalnej administracji

1. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych Windows.
2. Zdalna instalacja wszystkich wersji programów na stacjach roboczych NT 4.0 sp4/2000/XP Professional/ Vista/Windows7.
3. Do instalacji zdalnej i zarządzania zdalnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy
4. Komunikacja miedzy serwerem a klientami może być zabezpieczona hasłem.
5. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego
6. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej.
7. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych).
8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy.
9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
10. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.
11. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.
12. Możliwość importowania konfiguracji programu z wybranej stacji roboczej a następnie przesłanie (skopiowanie) jej na inną stację lub grupę stacji roboczych w sieci.
13. Możliwość zmiany konfiguracji na stacjach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).
14. Możliwość uruchomienia serwera zdalnej administracji na stacjach Windows NT 4.0 (Service Pack 6)/2000/XP/Vista/Windows 7 oraz na serwerach Windows NT 4.0 (Service Pack 6)//2000/2003/2008 – 32 i 64-bitowe systemy.
15. Możliwość uruchomienia centralnej konsoli zarządzającej na stacji roboczej Windows 2000/XP/Vista/Windows7, oraz na serwerach Windows 2000/2003/2008 - 32 i 64-bitowe systemy.
16. Możliwość wymuszenia konieczności uwierzytelniania stacji roboczych przed

połączeniem się z serwerem zarządzającym. Uwierzytelnianie przy pomocy zdefiniowanego na serwerze hasła.

17. Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie żadnych dodatkowych baz typu MSDE lub MS SQL. Serwer centralnej administracji musi mieć własną wbudowaną bazę w pełni kompatybilną z formatem bazy danych programu Microsoft Access.
18. Serwer centralnej administracji powinien oferować administratorowi możliwość współpracy przynajmniej z trzema zewnętrznymi motorami baz danych w tym minimum z: Microsoft SQL Server, MySQL Server oraz Oracle.
19. Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie dodatkowych aplikacji takich jak Internet Information Service (IIS) czy Apache.
20. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) w formacie HTML lub CSV.
21. Możliwość tworzenia hierarchicznej struktury serwerów zarządzających i replikowania informacji pomiędzy nimi w taki sposób, aby nadrzędny serwer miał wgląd w swoje stacje robocze i we wszystkie stacje robocze serwerów podrzędnych (struktura drzewiasta).
22. Serwer centralnej administracji powinien oferować funkcjonalność synchronizacji grup komputerów z drzewem Active Directory. Synchronizacja ta, powinna automatycznie umieszczać komputery należące do zadanych grup w AD do odpowiadających im grup w programie. Funkcjonalność ta nie powinna wymagać instalacji serwera centralnej administracji na komputerze pełniącym funkcję kontrolera domeny.
23. Serwer centralnej administracji powinien umożliwiać definiowanie różnych kryteriów wobec podłączonych do niego klientów (w tym minimum przynależność do grupy roboczej, przynależność do domeny, adres IP, adres sieci/podsieci, zakres adresów IP, nazwa hosta, przynależność do grupy, brak przynależności do grupy). Po spełnieniu zadanego kryterium lub kilku z nich stacja powinna otrzymać odpowiednią konfigurację.
24. Serwer centralnej administracji powinien być wyposażony w mechanizm informowania administratora o wykryciu nieprawidłowości w funkcjonowaniu oprogramowania zainstalowanego na klientach w tym przynajmniej informowaniu o: wygaśnięciu licencji na oprogramowanie, o tym że zdefiniowany procent z pośród wszystkich stacji podłączonych do serwera ma nieaktywną ochronę oraz że niektórzy z klientów podłączonych do serwera oczekują na ponowne uruchomienie po aktualizacji do nowej wersji oprogramowania.
25. Serwer centralnej administracji powinien być wyposażony w wygodny mechanizm zarządzania licencjami, który umożliwi sumowanie liczby licencji nabytych przez użytkownika. Dodatkowo serwer powinien informować o tym, ilu stanowiskową licencję posiada użytkownik i stale nadzorować ile licencji spośród puli nie zostało jeszcze wykorzystanych.
26. W sytuacji, gdy użytkownik wykorzysta wszystkie licencje, które posiada po zakupie oprogramowania, administrator po zalogowaniu się do serwera poprzez konsolę administracyjną powinien zostać poinformowany o tym fakcie za pomocą okna informacyjnego.
27. Możliwość tworzenia repozytorium aktualizacji na serwerze centralnego zarządzania i udostępniania go przez wbudowany serwer http.
28. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
29. Dostęp do kwarantanny klienta z poziomu systemu zdalnego zarządzania.
30. Możliwość przywrócenia lub pobrania zainfekowanego pliku ze stacji klienckiej przy wykorzystaniu zdalnej administracji
31. Administrator powinien mieć możliwość przywrócenia i wyłączenia ze skanowania pliku pobranego z kwarantanny stacji klienckiej
32. Podczas przywracania pliku, administrator powinien mieć możliwość zdefiniowania kryteriów dla plików które zostaną przywrócone w tym minimum: zakres czasu z

dokładnością co do minuty kiedy wykryto daną infekcję, nazwa danego zagrożenia, dokładna nazwa wykrytego obiektu oraz zakres minimalnej i maksymalnej wielkości pliku z dokładnością do jednego bajta.

33. Możliwość utworzenia grup, do których przynależność jest aplikowana dynamicznie na podstawie zmieniających się parametrów klientów w tym minimum w oparciu o: wersję bazy sygnatur wirusów, maskę wersji bazy sygnatur wirusów, nazwę zainstalowanej aplikacji, dokładną wersję zainstalowanej aplikacji, przynależność do domeny lub grupy roboczej, przynależność do serwera zdalnego zarządzania, przynależności lub jej braku do grup statycznych, nazwę komputera lub jej maskę, adres IP, zakres adresów IP, przypisaną politykę, czas ostatniego połączenia z systemem centralnej administracji, oczekiwania na restart, ostatnie zdarzenie związane z wirusem, ostatnie zdarzenie związane z usługą programu lub jego procesem, ostatnie zdarzenie związane ze skanowaniem na żądanie oraz z nieudanym leczeniem podczas takiego skanowania, maską wersji systemu operacyjnego oraz flagą klienta mobilnego.
34. Podczas tworzenia grup dynamicznych, parametry dla klientów można dowolnie łączyć oraz dokonywać wykluczeń pomiędzy nimi.
35. Utworzone grupy dynamiczne mogą współpracować z grupami statycznymi.