OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia są sukcesywne dostawy licencji oprogramowania antywirusowego dla stacji roboczych

CPV: 48761000-0 – pakiety oprogramowania antywirusowego

1. Przedmiotem zamówienia jest świadczenie usługi dostawy sukcesywnej 6187 sztuk licencji oprogramowania antywirusowego dla stacji roboczych, serwerów, urządzeń mobilnych.
2. Rozwiązanie antywirusowe musi pozwalać na centralne zarządzanie poszczególnymi antywirusami zainstalowanymi na stacjach roboczych oraz serwerach, poprzez darmowy server/panel administratora.

Wymagania dotyczące rozwiązania antywirusowego

Wymagane:	**Minimalne wymagania które musi zapewniać oprogramowanie antywirusowe**
Wymagania ogólne:	1. Pełne wsparcie dla systemu Windows XP/Vista/7/8/8.1/10. 2. Pełne wsparcie dla systemu Windows Server 2003/2008/2008R2/2012/2012R2/2016 3. Pełne wsparcie dla systemów Linux, Mac, Android 4. Wsparcie dla 32- i 64-bitowej wersji systemu Windows. 5. Wersja programu dla stacji roboczych, serwerów Windows dostępna zarówno w języku polskim jak i angielskim. 6. Pomoc w programie (help) i dokumentacja do programu w języku polskim.
Wymagania dotyczące ochrony antywirusowej i antyspyware:	1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. Instalacja klientów dla systemów operacyjnych Windows, Linux, Mac oraz Android. 2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 3. Wbudowana technologia do ochrony przed rootkitami. 4. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 5. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 6. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 7. Możliwość ustawienia automatycznego skanowania dysków przenośnych. 8. Skanowanie plików spakowanych i skompresowanych. 9. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 10. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 11. 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. 12. Wbudowany konektor dla programu pocztowego firmy Microsoft.

Wymagane:	**Minimalne wymagania które musi zapewniać oprogramowanie antywirusowe**
	13. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 14. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 15. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie. 16. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła. 17. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło. 18. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 19. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 20. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych 21. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 22. Program ma 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. 23. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. 24. Aktualizacja baz wirusów i innych zagrożeń dostępna z nośnika pamięci. 25. Aplikacja musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. 26. Aplikacja musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback). 27. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 28. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania. 29. Aplikacja musi być wyposażona w funkcjonalność zapory osobistej (Personal Firewall). 30. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
Wymagania dotyczące	1. Centralna instalacja programów służących do ochrony stacji roboczych.

Wymagane:	**Minimalne wymagania które musi zapewniać oprogramowanie antywirusowe**
centralnego zarządzania:	2. Centralne zarządzanie programami służącymi do ochrony stacji roboczych. 3. Centralna instalacja oprogramowania na końcówkach (stacjach roboczych). 4. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. 5. Możliwość uruchomienia centralnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej. 6. 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). 7. 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. 8. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu. 9. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych. 10. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów. 11. 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). 12. Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) w formacie HTML lub CSV. 13. Serwer centralnej administracji ma oferować funkcjonalność synchronizacji grup komputerów z drzewem Active Directory. Po synchronizacji automatycznie są umieszczane komputery należące do zadanych grup w AD do odpowiadających im grup w programie. Funkcjonalność ta nie może wymagać instalacji serwera centralnej administracji na komputerze pełniącym funkcję kontrolera domeny. 14. Serwer centralnej administracji ma 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 ma otrzymać odpowiednią konfigurację. 15. Serwer centralnej administracji ma 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. 16. Możliwość tworzenia repozytorium aktualizacji na serwerze centralnego

Wymagane:	Minimalne wymagania które musi zapewniać oprogramowanie antywirusowe
	zarządzania i udostępniania go przez wbudowany serwer http. 17. Możliwość definiowania administratorów o określonych prawach do zarządzania serwerem administracji centralnej (w tym możliwość utworzenia administratora z pełnymi uprawnieniami lub uprawnienia tylko do odczytu). 18. Możliwość synchronizowania użytkowników z Active Directory w celu nadania uprawnień administracyjnych do serwera centralnego zarządzania. 19. Możliwość przywrócenia baz sygnatur wirusów wstecz (tzw. Rollback). 20. Aplikacja musi mieć możliwość przygotowania paczki instalacyjnej dla stacji klienckiej, która będzie pozbawiona wybranej funkcjonalności.