**Załącznik nr 1.2**

**Szczegółowy opis przedmiotu zamówienia do Część 3- Dostawa 57 licencji AV (oprogramowania komputerowego)**

|  |  |
| --- | --- |
| Nazwa | Wymagane parametry techniczne –  **Wymagania jakościowe odnoszące się do głównych elementów składających się na przedmiot zamówienia** |
| 1. Zastosowanie | Oprogramowanie antywirusowe do ochrony komputerów, laptopów, serwerów plików i baz danych. |
| 1. Wsparcie dla systemów | Microsoft Windows Server 2008 R2 i nowszych.  Microsoft Windows 7 SP1 Pro i nowszych. |
| 1. Ochrona antywirusowa i antyspyware | Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.  Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi  Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.  Wbudowana technologia do ochrony przed rootkitami.  Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.  Możliwość wywołania skanowania "na żądanie".  Możliwość skanowania dysków sieciowych podłączonych do komputera i pamięci USB (dopuszczalne lokalnie skanowanie) .  Skanowanie plików spakowanych i skompresowanych.  Możliwość dodawania wykluczeni na podstawie :Plik, Folder, Proces,  Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programów pocztowych.  Automatyczna integracja skanera z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. (dopuszczalna wtyczka do programu pocztowego)  Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.  Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator.  Automatyczna integracja z najpopularniejszymi przeglądarkami internetowymi bez konieczności zmian w konfiguracji.  Program umożliwia skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.  Program skanuje ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki  Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program będzie pytał o hasło.  W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.  Automatyczna aktualizacja baz wirusów i innych zagrożeń.  Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.  Praca programu musi być niezauważalna dla użytkownika. (tryb cichy)  Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń  Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.  Możliwość odblokowania ustawień programu po wpisaniu hasła  Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu.  Funkcja Ochrony danych konfigurowana zdalnie przez administratora.  Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego z konsoli lub na końcówce.  Możliwość tworzenia list sieci zaufanych.  Możliwość dezaktywacji funkcji zapory sieciowej na pewien czas.  Połączenie szyfrowane dla punktów końcowych Windows do serwera zarządzającego.  Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci.  Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware  Ochrona proaktywna oparta o maszynowe uczenie  Plik może zostać wysłany automatycznie lub ręcznie ze stacji roboczej jeżeli oprogramowanie uzna go za podejrzany  Wbudowany sandbox musi działać w trybie monitorowania i blokowania  Wbudowany sandbox musi posiadać opcję która pozwala na dodanie określonych wykluczeni.  Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych  Możliwość szybkiego podglądu otwartych incydentów, najczęstszych powiadomień, urządzeń które mają najczęściej problem. |
| 1. Skuteczność rozwiązań | Skuteczność rozwiązania potwierdzona nagrodami VB100 bądź AV-comparatives. |
| 1. Wsparcie | Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim oraz angielskim. |
| 1. Konsola zdalnej administracji | Konsola Cloud – serwer administracyjny po stronie producenta  Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.  Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego.  Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.  Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).  Możliwość utworzenia konta użytkownika z rolą administrator, gościa (podgląd ustawień)  Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.  Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.  Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej (nadrzędna) lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.  Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.  Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv  Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych  Możliwość dodania etykiety do stacji roboczej widzianej w konsoli.  Możliwość przechowywania kwarantanny.  W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.  Możliwość naprawy instalacji z poziomu konsoli w sieci lokalnej.  Możliwość podglądu raportu który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:  -Zarządzane punkty końcowe  -Aktualny zapas wolnych miejsc w licencji  Tworzenie osobnych polityk  Funkcja kontroli aplikacji pozwala na zablokowanie wybranych plików lub procesów przed dostępem do Internetu.  Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.  Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym.  Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, |
| 1. Licencja | Min 2 lata od momentu podpisania umowy |