Załącznik nr 2 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest przedłużenie aktualizacji i wsparcia technicznego dla systemu antywirusowego w ilości 244 licencji.

Lp.	Parametr	Charakterystyka
1	Nazwa aktualizowanego oprogramowania	Symantec Endpoint Protection w najnowszej wersji oferowanej przez producenta
2	Rodzaj licencjonowania	Aktualizacja licencji dla instytucji akademickich ze wsparciem na poziomie BASIC na okres co najmniej 1 roku umożliwiająca pobieranie aktualizacji i kontakt ze wsparciem producenta w dni robocze Daty ważności istniejących licencji: - 21-03-2017 – 174 licencje - 22-03-2017 – 70 licencji
3	Oprogramowanie alternatywne	Zamawiający dopuści rozwiązanie równoważne do eksploatowanego oprogramowania Symantec Endpoint Protection, pod warunkiem że będzie dostarczona nowa licencja ze wsparciem producenta na co najmniej 1 rok. Oferowane wsparcie powinno obejmować dostęp do najnowszych sygnatur dla poszczególnych modułów zabezpieczeń, aktualizacji składników oprogramowania oraz możliwość konsultacji telefonicznych z inżynierem producenta w standardowych godzinach pracy. Oprogramowanie musi posiadać następujące funkcjonalności: 1. Ochrona antywirusowa: - ochrona przed wirusami i programami typu spyware - ochronę przed nieznanymi zagrożeniami i atakami na nieznane luki w zabezpieczeniach - prewencyjne skanowania w poszukiwaniu aktywnych procesów wykazujących cechy destrukcyjne. - automatyczne skanowanie plików do których użytkownik ma dostęp oraz otwieranych, zapisywanych, kopiowanych, przenoszonych i wykonywanych, - możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według zaplanowanego harmonogramu, - możliwość uruchamiania skanowania pliku lub folderu z menu kontekstowego, - możliwość definiowania wielu zadań skanowania z różnymi ustawieniami, - możliwość blokowania dostępu użytkownika do ustawień automatycznej ochrony, - możliwość definiowania wyjątków skanowania dla plików, folderów, rozszerzeń plików oraz skanowania prewencyjnego, - możliwość przenoszenia zainfekowanych plików do kwarantanny, - możliwość podejmowania odpowiednich czynności przez użytkownika oraz administratora z poziomu konsoli systemu zarządzającego, - możliwość skanowania wychodzącej i przychodzącej poczty elektronicznej - SMTP, POP3, IMAP, - automatyczna integracja z klientami poczty MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird bez konieczności zamian w ich konfiguracji, - rejestracja zdarzeń związanych z infekcjami wirusowymi i spayware, potencjalnymi zagrożeniami oraz z zagrożeniami sieciowymi, - automatyczna rejestracja nieautoryzowanych prób zmian rejestrów dokonywanych przez użytkownika, - umożliwiać blokowanie dostępu do pliku autorun.inf na dyskach

		wymiennych oraz sieciowych, - opóźnianie skanowania zaplanowanego w sytuacji komputer przenośny jest zasilany z baterii, 2. Zapora sieciowa: - zabezpieczenie stacji klienckich przed atakami hakerów oraz nieautoryzowanymi próbami dostępu do komputerów i skanowaniem portów, - konfiguracja reguł zapory lokalnej w oparciu o protokoły ICMP,UDP, TCP, Ethernet, - konfiguracja zezwalanego i zabronionego ruchu w oparciu o takie informacje jak: interfejs sieciowy, protokół, stacja docelowa, aplikacja, - możliwość konfigurowania zapory sieciowej w taki sposób by możliwe było powiadamianie użytkownika o zablokowanych aplikacjach. Musi istnieć możliwość dodania własnego komunikatu, - możliwość definiowania różnych działań automatycznej ochrony w odpowiedzi na różne zagrożenia dotyczące systemu plików oraz poczty elektronicznej (czyszczenie, kwarantanna, usunięcie zagrożenia), - możliwość ograniczania dostępu do sieci dla poszczególnych aplikacji, - wykrywanie skanowania portów i ataków typu DoS oraz automatyczne blokowanie adresu IP atakującego na określony czas, - możliwość pozostawienia bez zmian i wyłączania zapory wbudowanej w systemach Windows. 3. Zapobieganie włamaniom - ochrona przed zagrożeniami sieciowymi poprzez konfigurowaną dwukierunkową zaporę sieciową oraz mechanizm IPS, - automatyczna aktualizacja sygnatur zagrożeń sieciowych udostępnianych przez producenta oprogramowania, - możliwość definiowania własnych sygnatur zagrożeń, 4. Kontrola urządzeń i aplikacji: - kontrolę dostępu do nośników wymiennych USB, CD/DVD z możliwością blokowania, - możliwość blokowania dostępu do urządzeń typu drukarka skaner, czytniki kart, urządzenia HID, interfejsy sieciowe i bluetooth, - możliwość blokowania uruchamiania programów z nośników wymiennych, - możliwość rejestrowania lub blokowania zapisu na nośnikach USB, - możliwość blokowania dostępu do plików systemowych i skryptów (np. autorun.ini, blokada modyfikacji pliku hosts i innych plików systemowych), 5. Obsługiwane systemy operacyjne operacyjnych i metody instalacji: - możliwość instalacji w 32 i 64 bitowych systemach Windows XP, 7, 8, Serwer 2003/2008 oraz Linux - Interfejs użytkownika oraz pomoc w języku polskim (co najmniej dla instalacji w systemach Windows), - instalację zarządzaną oraz nie zarządzaną, - instalacja centralnego modułu zarządzania stacjami klienckimi musi być możliwa w tym samym systemie operacyjnym co moduł zarządzania oprogramowania Symantec Endpoint Ptotection i nie może ograniczać jego funkcjonalności, - automatyczną aktualizację sygnatur udostępnianych przez producenta za pomocą Internetu, - możliwość aktualizację sygnatur „offline” na komputerach nie posiadających połączenia z Internetem, 6 Centralne zarządzanie instalacjami klienckimi: - zdalną instalację oprogramowania klienckiego w postaci instalacji „wypychanej” oraz instalacji użytkownika (na żądanie), - zdalną instalację dodatkowych modułów oprogramowania klienckiego, - współpracę z kontrolerem domeny ActiveDirectory, - wykrywanie komputerów bez zainstalowanego oprogramowania klienckiego, z oprogramowaniem nie zarządzanym lub z nieaktualnymi sygnaturami, w różnych segmentach sieci,

		- zdalne konfigurowanie wszystkich parametrów oprogramowania klienckiego, - możliwość definiowania ustawień dla pojedynczych komputerów oraz grup, - centralną rejestrację wszystkich zdarzeń występujących na komputerach zarządzanych, - podgląd szczegółów zarejestrowanego incydentu na dowolnym z zarządzanych komputerów, - generowanie zastawień i statystyk dotyczących występujących zagrożeń wraz z szacowaniem średniego poziomu bezpieczeństwa, - informowanie o zagrożeniach, które nie zostały usunięte, wyczyszczone, - wykrywanie modyfikacji oprogramowania klienckiego przez sprawdzenie integralności hosta, - automatyczną i na żądanie aktualizację zasad bezpieczeństwa na komputerach klienckich, - sprawdzenie aktualności zasad bezpieczeństwa na komputerach klienckich, - automatyczne lub na żądanie włączenie automatycznej ochrony w przypadku kiedy użytkownik ją wyłączył, - automatyczne wymuszanie pobierania nowych definicji wirusów na komputerach klienckich, - konfigurację powiadomień email dla administratora przy wystąpieniu poszczególnych zagrożeń, - zarządzanie zdalne zagrożeniami przeniesionych do kwarantanny – przywracanie pliku do pierwotnej lokalizacji, ponowne skanowanie i usuwanie z kwarantanny, - przesyłanie potencjalnie zainfekowanych plików do laboratorium producenta w celu poddania ich analizie, Ponadto Dostawca rozwiązania równoważnego zobowiązany jest do: - przeprowadzenia szkoleń co najmniej 2 pracowników Zamawiającego, w zakresie instalacji i konfiguracji wszystkich wyżej opisanych funkcjonalności oprogramowania wymaganych przez Zamawiającego, - wykonania deinstalacji oprogramowania Symantec Endpoint Ptotection oraz instalacji nowego programu antywirusowego, na stanowiskach objętych licencją. Czynności instalacyjne mogą być wykonywane w obecności właściwego administratora, w godzinach 8:00 16:00, w dni robocze od poniedziałku do piątku.