Załącznik nr 2 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedłużenie aktualizacji i wsparcia technicznego dla systemu antywirusowego - 244 licencji.

Lp.	Parametr	Charakterystyka
1	Nazwa aktualizowanego oprogramowania	Symantec/Broadcom 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: - 18-10-2020 – 64 licencje, numer seryjny M0318356164 - 16-11-2020 – 75 licencji, numer seryjny M0240252748 - 19-12-2020 - 16 licencji, numer seryjny M5939647716 - 22-12-2020 - 40 licencji, numer seryjny M7143147993
3	Oprogramowanie alternatywne	Zamawiający dopuści rozwiązanie równoważne do eksploatowanego oprogramowania Symantec/Broadcom Endpoint Protection, pod warunkiem że będzie dostarczona nowa licencja ze wsparciem producenta na co najmniej 1 rok od dnia zakończenia ostatniej licencji (22-12-2020), przy czym ochrona musi być dostępna dla licencji wygasających wcześniej. 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. Licencja musi pozwalać na instalację na co najmniej 20 systemach serwerowych. Oprogramowanie musi posiadać następujące funkcjonalności: 1. Ochrona antywirusowa: - ochrona przed wirusami, trojanami, robakami, - ochronę przed nieznanymi zagrożeniami i atakami na nieznane luki w zabezpieczeniach, - wykrywanie i blokowanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp., - prewencyjne skanowania w poszukiwaniu aktywnych procesów wykazujących cechy destrukcyjne. - automatyczne skanowanie plików które użytkownik przetwarza: otwiera, zapisuje, kopiuje, przenosi lub uruchamia, - skanowanie zawartości plików skompresowanych, - 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 definiowania wyjątków skanowania dla: plików, folderów, rozszerzeń plików, - automatyczne przenoszenie do kwarantanny zainfekowanych plików do kwarantanny z możliwością wykonania ponownej kontroli antywirusowej oraz przywrócenia do pierwotnej lokalizacji, - możliwość podejmowania odpowiednich czynności przez użytkownika oraz administratora z poziomu konsoli systemu zarządzającego, - możliwość skanowania w czasie rzeczywistym poczty przychodzącej wykorzystującej protokoły POP3 oraz IMAP,

		- automatyczna integracja z klientami poczty MS Outlook, Windows Mail, Mozilla Thunderbird bez konieczności zamian w ich konfiguracji, - rejestracja zdarzeń związanych z infekcjami wirusowymi i spayware, potencjalnymi zagrożeniami oraz z zagrożeniami sieciowymi, - możliwość blokowania dostępu użytkownika do ustawień automatycznej ochrony, - opóźnianie skanowania zaplanowanego w sytuacji komputer przenośny jest zasilany z baterii, - zapobieganie modyfikacji plików systemowych (np. blokowanie modyfikacji hosts) i uruchamiania skryptów (np. blokowanie przetwarzania autorun.ini), - kontrolę dostępu do nośników wymiennych USB, CD/DVD z możliwością blokowania, - możliwość blokowania dostępu do urządzeń typu czytniki kart, pamięci USB, i innych urządzeń typu HID, - możliwość blokowania uruchamiania programów z nośników wymiennych, 2. Ochrona sieciowa: - zabezpieczenie stacji klienckich przed atakami hakerów oraz nieautoryzowanymi próbami dostępu do komputerów i skanowaniem portów za pomocą konfigurowanej dwukierunkowej zapory sieciowej oraz mechanizm IPS, - konfiguracja reguł zapory lokalnej w oparciu o protokoły IP, ICMP,UDP, TCP, Ethernet, - konfiguracja zezwalanego i zabronionego ruchu w oparciu o takie informacje jak: interfejs sieciowy, protokół, stacja źródłowa / docelowa, aplikacja, - możliwość ograniczania dostępu do sieci dla poszczególnych aplikacji, - wykrywanie skanowania portów i ataków typu DoS oraz automatyczne blokowanie adresu IP atakującego na określony czas, - automatyczna aktualizacja sygnatur zagrożeń sieciowych udostępnianych przez producenta oprogramowania, - możliwość definiowania własnych zasad reakcji na zagrożenia, - możliwość wyłączania zapory wbudowanej w systemach Windows. 3. Obsługiwane systemy operacyjne operacyjnych i metody instalacji: - obsługa 32 i 64 bitowych systemów Windows 7, 8, 10, Serwer 2008R2/2019, Linux oraz macOS, - możliwość instalacji starszych wersji oprogramowania antywirusowego w systemach Windows XP i Vista, - 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 Manager i nie może ograniczać jego funkcjonalności, - automatyczną aktualizację sygnatur udostępnianych przez producenta za pomocą Internetu, - możliwość aktualizacji sygnatur „offline” na komputerach nie posiadających połączenia z Internetem, 4 Funkcjonalności centralnego zarządzania systemem antywirusowym. W ramach licencji musi być dostępne oprogramowanie do centralnego zarządzania oprogramowaniem antywirusowym do instalacji w środowisku Windows, Linux lub kompletnej maszyny wirtualnej do instalacji w środowisku VMWare posiadające następujące funkcjonalności: - zdalna instalacja oprogramowania antywirusowego w postaci instalacji „wypychanej” oraz instalacji użytkownika (na żądanie) – przygotowana paczka instalacyjna posiadająca wszystkie niezbędne parametry

		komunikacyjne, - współpracę z kontrolerem domeny ActiveDirectory, - wykrywanie komputerów bez zainstalowanego oprogramowania antywirusowego, z oprogramowaniem nie zarządzanym lub z nieaktualnymi sygnaturami, w różnych segmentach sieci, - zdalne konfigurowanie wszystkich parametrów oprogramowania antywirusowego, - możliwość definiowania parametrów dla pojedynczych komputerów oraz grup komputerów, - możliwość definiowania działań automatycznej ochrony w odpowiedzi na zaistniałe rodzaje zagrożeń dotyczących ochrony antywirusowej oraz zapory sieciowej (np. czyszczenie, kwarantanna, rejestrowanie, usunięcie zagrożenia, blokowanie dostępu), - centralną rejestrację zdarzeń dotyczących bezpieczeństwa występujących na zarządzanych komputerach, - podgląd szczegółów zarejestrowanego incydentu, który wystąpił na dowolnym z zarządzanych komputerów, - generowanie zastawień i statystyk dotyczących występujących zdarzeń, zagrożeń, ilości komputerów i stanu zainstalowanego na nich oprogramowania antywirusowego, - informowanie o zagrożeniach, które nie zostały usunięte, wyczyszczone, - automatyczną aktualizację oraz na żądanie zasad i sygnatur bezpieczeństwa na chronionych komputerach, - sprawdzenie aktualności zasad bezpieczeństwa na komputerach z zainstalowanym oprogramowaniem antywirusowym, - automatyczne lub na żądanie włączenie automatycznej ochrony w przypadku kiedy użytkownik ją wyłączył, - automatyczne wymuszanie pobierania nowych definicji zagrożeń na komputerach klienckich, - generowanie raportów związanych ze stanem ochrony na poszczególnych urządzeniach, rodzajów występujących zagrożeń, przeprowadzonych zadań skanowania i zdarzeń systemowych, - monitorowanie zagrożeń przeniesionych do kwarantanny, - przesyłanie potencjalnie zainfekowanych plików do laboratorium producenta w celu poddania ich analizie, - możliwość generowania wiadomości email do administratorów w przypadku wystąpienia zagrożeń i innych zdarzeń systemowych. Ponadto Dostawca rozwiązania równoważnego zobowiązany jest do przeprowadzenia szkoleń co najmniej 2 administratorów Zamawiającego, w zakresie instalacji i konfiguracji wyżej opisanych funkcjonalności oprogramowania wymaganych przez Zamawiającego lub zgodnie z programem szkoleniowym producenta oprogramowania. Szkolenie może być przeprowadzone przez Wykonawcę lub inny wskazany podmiot metodą stacjonarną lub zdalną, przy czym środowisko dydaktyczne zapewnia podmiot szkolący. Szkolenie metodą zdalną powinno odbywać się w sesjach nie dłuższych niż 4 godziny dziennie. Instruktor będzie udzielał wsparcia osobom szkolonym przez co najmniej 14 dni po zakończeniu kursu.