Załącznik nr 1
Szczegółowy opis przedmiotu zamówienia

Przedmiot zamówienia obejmuje zakup odnowienia subskrypcji Veeam Backup Essentials Standard, serwisu FortiCare 8x5 oraz licencji oprogramowania antywirusowego wraz z aktualizacją bazy wirusów na potrzeby Regionalnej Dyrekcji Ochrony Środowiska w Białymstoku. Przedmiot zamówienia został podzielony na dwa zadania:

1. Zadanie 1 obejmuje:
   1) odnowienie wsparcia technicznego oprogramowania Veeam Backup Essentials Standard for Hyper-V (4 gniazda procesorowe) na okres 12 miesięcy (P/N: V-ESSSTD-HS-P01AR-00), obecna licencja wygasa 30 marca 2017 r
   2) odnowienie serwisu FortiCare FC-10-P0223-311-02-12 obejmujące urządzenie FortiAP-221B (FAP-221B), systemem wymiany 8x5, wsparcie techniczne oraz dające możliwość aktualizacji oprogramowania – licencja dla dwóch urządzeń na okres 12 miesięcy.
2. Zadanie 2 obejmuje:
   1) dostawę licencji wielostanowiskowej na oprogramowanie antywirusowe wraz z aktualizacją bazy wirusów na okres 36 miesięcy.

Wykonawca może złożyć ofertę na jedno lub dwa zadania.

Zadanie 1.

Oferta wykonawcy powinna obejmować całość przedmiotu zamówienia objętego zadaniem 1.

Zadanie 2.

Wymagania dotyczące oprogramowania antywirusowego:

Zamawiający obecnie posiada licencję wielostanowiskową oprogramowania Kaspersky Endpoint Security for Business - Select na 60 stanowisk, która wygasa 24 lutego 2017 r.

Dostarczone oprogramowanie ma chronić systemy użytkowane przez zamawiającego:

- 58 fizycznych stacji roboczych z systemem Windows 7/8.1/10 (x64);
- 2 wirtualne serwery plików z systemem Windows Server 2008 i 2012, działające na hoście Microsoft Hyper-V 3.0.

Licencja ma obowiązywać przez okres 36 miesięcy, począwszy od 24 lutego 2017 r.

Wymagania wspólne dla ochrony stacji roboczych oraz serwerów plików:

1. Ochrona antywirusowa i antyspyware w czasie rzeczywistym
2. Możliwość skanowania z wykorzystaniem analizy heurystycznej oraz sygnatur wirusów
3. Możliwość wykonania skanowania według harmonogramu (codziennie o określonej godzinie lub w wybrane dni tygodnia) oraz na żądanie
4. Automatyczne skanowanie systemu w trakcie bezczynności chronionego urządzenia

5. Możliwość aktualizacji bazy wirusów z Internetu lub z lokalnego serwera aktualizacji oraz aktualizacji bazy w trybie offline
6. Zdalna instalacja aplikacji, uruchamianie zadań, zbieranie logów
7. Możliwość definiowania wykluczeń skanowania na podstawie rozszerzenia plików oraz według określonej ścieżki do folderu lub pliku
8. Producent udostępnia gotowy obraz płyty lub narzędzie do przygotowania awaryjnego nośnika CD/DVD/USB, z którego będzie możliwe uruchomienie zainfekowanego urządzenia w celu przeskanowanie i usunięcia wirusów
9. Możliwość przeniesienia zainfekowanych plików do kwarantanny
10. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, zadań skanowania, aktualizacji baz wirusów i samego oprogramowania

Wymagania dodatkowe dotyczące klienta instalowanego na stacjach roboczych:

1. Skanowanie protokołów: HTTP, POP3, IMAP
2. Ochrona programów pocztowych: Microsoft Outlook (2007, 2010, 2013, 2016) oraz Mozilla Thunderbird 45
3. Możliwość automatycznego skanowania nośników wymiennych (pendrive, CD/DVD, dyski USB, karty pamięci) po podłączeniu do komputera
4. Automatyczne wykrywanie i usuwanie innego oprogramowania antywirusowego podczas instalacji
5. GUI w polskiej wersji językowej
6. Możliwość wstrzymania ochrony antywirusowej na określony czas z poziomu GUI po podaniu hasła

Wymagania dotyczące serwera zarządzającego:

1. Serwer dostępny, jako Virtual Appliance dla hosta Hyper-V lub jako aplikacja do zainstalowania w systemie Windows Server 2008/2012
2. Konsola serwera dostępna przez przeglądarkę www lub jako aplikacja do zainstalowania w systemie Windows 7/8.1/10 64bit
3. Integracja z domeną Active Directory umożliwiająca logowanie administratora do konsoli z wykorzystaniem poświadczeń domenowych oraz widok struktury lasu (OU oraz grupy domenowe)
4. Zdalna instalacja oprogramowania antywirusowego na stacjach roboczych i serwerach plików
5. Pełna administracja zdalnymi klientami za pomocą konsoli administracyjnej (zarządzanie wszystkimi ustawieniami programu antywirusowego, ustanawianie polityk bezpieczeństwa, zbieranie logów, uruchamianie zadań skanowania)
6. Możliwość wyświetlenia informacji dotyczących zarządzanego urządzenia, takich jak: wersja programu antywirusowego i bazy wirusów, aktualna konfiguracja programu, wyniki skanowania, wykryte zagrożenia

7. Wbudowane narzędzie diagnostyczne generujące szczegółowy raport dotyczący zarządzanego urządzenia zawierający: listę zainstalowanych aplikacji oraz usług systemowych, informacje o systemie operacyjnym, sprzęcie, aktywnych procesach i połączeniach
8. Centralne zarządzanie kwarantanną zarządzanych urządzeń
9. Możliwość przywrócenia lub usunięcia zainfekowanego pliku z kwarantanny stacji klienckiej
10. Automatyczne powiadomienia o zagrożeniach wykrytych na stacjach roboczych i serwerach (email, wpis do dziennika systemu Windows oraz do konsoli serwera zarządzającego)
11. Tworzenie raportów zawierających statystyki dotyczące wykrytych zagrożeń
12. Możliwość konfiguracji, jako wewnętrzny serwer aktualizacji pobierający aktualizacje sygnatur wirusów z serwerów producenta w celu dystrybucji do stacji klienckich
13. Identyfikacja niezarządzanych maszyn w domenie Windows Active Directory
14. Możliwość samodzielnego logicznego grupowania klientów jak również wykorzystania grup zdefiniowanych w domenie Active Directory oraz przypisywania do grup określonych zasad bezpieczeństwa.