OPIS PRZEDMIOTU ZAMÓWIENIA

I. Przedmiot zamówienia obejmuje:

1. zakup **dla 100 użytkowników** licencji na program antywirusowy w wersji z ochroną połączenia internetowego (zapewniający ochronę przed wszelakiego rodzaju szkodliwym oprogramowaniem - wirusami, robakami, trojanami oraz komponentami szpiegującymi, z ochroną poczty e-mail) na okres 36 miesięcy licząc od dnia 1 czerwca 2017r., **wraz z pełną automatyczną subskrypcją aktualizacji baz wirusów i innych zagrożeń w tym okresie**, oraz
2. zakup licencji oprogramowania antywirusowego **dla 20 użytkowników urządzeń mobilnych (smartfon, tablet) z systemem Android** na okres 36 miesięcy, **wraz z pełną automatyczną subskrypcją aktualizacji baz wirusów i innych zagrożeń w tym okresie.**

II. Minimalne wymagania techniczne, funkcjonalne i użytkowe:

1) System umożliwia:
   a) automatyczną (zdalną) instalację na stacjach klienckich, bez dostępu do Internetu;
   b) automatyczną dystrybucję bazy sygnatur wirusów i aktualizacji komponentów programu w sieci wydzielonej, bez dostępu do Internetu (funkcjonalność serwera kopii dystrybucyjnej);
2) System posiada wbudowane narzędzie do analizy i gromadzenia wszystkich ważnych informacji o danym komputerze, bez konieczności korzystania z żadnych zewnętrznych stron internetowych, w szczególności o następujących funkcjonalnościach:
   a) gromadzenie informacji o aktywnych procesach, stanowiących zagrożenie dla komputera lub mogących być przyczyną jego nieprawidłowej pracy;
   b) możliwość selekcji i grupowania wszystkich procesów wg kryterium prawdopodobieństwa zagrożenia, jakie mogą powodować;
   c) możliwość określenia przyczyn błędnej pracy systemu, w tym m.in. tych powiązanych z działaniem złośliwych programów, które niezauważenie dla użytkownika przedostały się do systemu;
   d) możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach;
   e) konsola zarządzająca dostępna z poziomu przeglądarki;
   f) możliwość automatycznego wykrywania i usuwania innego oprogramowania antywirusowego podczas instalacji;
   g) możliwość ukrycia interfejsu przed użytkownikiem końcowym;
   h) program posiada kwarantannę spyware oraz riskware;
   i) program z Menu Start pozwala stworzyć plik diagnostyczny do analizy problemów;
   j) program pozwala z interfejsu graficznego użytkownika wysłać próbkę wirusa bezpośrednio do laboratorium antywirusowego producenta;
   k) program posiada narzędzie ręcznej aktualizacji stacji roboczych we wszystkich sygnaturach dla poszczególnych silników skanujących;
   l) automatyczne powiadamianie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem, czy stacja robocza jest odpowiednio zabezpieczona;
   m) skanowanie przez program na komputerze klienckim przychodzącej i wychodzącej poczty elektronicznej bez konieczności instalowania dodatkowych programów/modułów; w programach pocztowych nie modyfikowane są ustawienia konta, tj. serwera POP3, SMTP i IMAP; obsługa i wsparcie techniczne dla m.in. MS Outlook Express, MS Outlook, Mozilla, Netscape Mail;

n) program posiada wsparcie do filtrowania protokołu IPv6;
o) automatyczna kwarantanna blokująca ruch przychodzących i wychodzących realizowana na poziomie oferowanego oprogramowania, włączająca się w momencie, gdy stacja robocza posiada stare sygnatury antywirusowe.

3) Wbudowane dwa niezależne moduły heurystyczne - jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej i/lub obu metod jednocześnie.
4) Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
5) Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS - Host Intrusion Prevention System Host) lub równoważne rozwiązanie.
6) Moduł HIPS musi posiadać możliwość pracy w jednym z czterech trybów:
   a) tryb automatyczny z regułami gdzie aplikacja automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika;
   b) tryb interaktywny, w którym to aplikacja pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie;
   c) tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika;
   d) tryb uczenia się, w którym aplikacja uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu aplikacja musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
7) Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
8) Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
9) System umożliwia całkowitą, niekolidującą z pracą systemu operacyjnego i automatyczną deinstalację systemu na stacji klienckiej.
10) Do instalacji serwera centralnej administracji (konsoli administracyjnej) nie jest wymagane zainstalowanie żadnych dodatkowych baz typu MSDE lub MS SQL. Serwer centralnej administracji musi mieć własną wbudowaną bazę danych.
11) System musi być kompatybilny z systemami operacyjnymi: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10.
12) Wsparcie dla 32- i 64-bitowej wersji systemu Windows;
13) Wersja programu dla stacji roboczych Windows dostępna w języku polskim
14) Konsola administracyjna dostępna w języku polskim.
15) Dokumentacja do oprogramowania na stację roboczą oraz konsolę administracyjną w języku polskim (może być w postaci elektronicznej).