Załącznik nr 1 - Opis przedmiotu zamówienia i elementów równoważności oprogramowania za pomocą cech funkcjonalno-użytkowych.

Programy antywirusowe, zabezpieczające i antyspamowe

LP	NAZWA LICENCJI*		Liczba licencji/nośników
1	SymantecEndPoint Protection 14.0 STD lic Gov Band A firmy Symantec Corporation lub równoważne	pełna wersja 2 YR Maitenance	49
		upgrade 2YR Maintenance	81
		renewal 2YR Maintenance	95
		2YR Maintenance	259
		pełna wersja 1 YR Maitenance	0**
		upgrade 1YR Maintenance	0**
		1YR Maintenance	0**
2	Kaspersky Endpoint Security for Business Select firmy Kaspersky Lab lub równoważne	pełna wersja z 2 letnią aktualizacją	103
		upgrade z 2 letnią aktualizacją	1659
		pełna wersja z roczną aktualizacją	25
		upgrade z roczną aktualizacją	0**
3	ESET Endpoint Antivirus Suite firmy ESET lub równoważne	pełna wersja z 2 letnią aktualizacją	317
		upgrade z 2 letnią aktualizacją	228
		pełna wersja z roczną aktualizacją	54
		upgrade z roczną aktualizacją	23
4	ESET Endpoint Security Suite firmy ESET lub równoważne	pełna wersja z 2 letnią aktualizacją	272
		upgrade z 2 letnią aktualizacją	320
		pełna wersja z roczną aktualizacją	27
		upgrade z roczną aktualizacją	0**
5	ESET Endpoint Security for Android firmy ESET lub równoważne	pełna wersja z 3 letnią aktualizacją	266

UWAGA: Ważność abonamentu wg Załącznika nr 3 do umowy.

***licencje i nośniki dostarczone na mocy umowy będą należały do grupy najnowszych wersji i zawierały wszelkie wprowadzone w ostatnim okresie ulepszenia, z wyjątkiem przypadków, w których umowa licencyjna producenta określa inaczej**

**** Zamawiający w zamówieniu podstawowym nie dokonuje zakupu przedmiotowego oprogramowania ale zastrzega taką możliwość przy skorzystaniu z prawa opcji.**

Załącznik nr 1 - Opis przedmiotu zamówienia i elementów równoważności oprogramowania za pomocą cech funkcjonalno-użytkowych.

Poniższe opisy zawierają minimalne parametry funkcjonalno użytkowe zamawianego oprogramowania.

Wymienione oprogramowanie antywirusowe powinno posiadać zaawansowaną ochroną przed zagrożeniami, zapewniając najwyższy stopień ochrony komputerów przenośnych, stacji roboczych i serwerów przed destrukcyjnym oprogramowaniem w jednostkach organizacyjnych LP.

Minimalne wymagania systemowe programów:

1. Windows 10 i Windows 10 Pro (wersje 32- i 64-bitowe)
2. Windows Vista (32-bit, 64-bit)
3. Windows 7 (32-bit, 64-bit)
4. Windows 8 i Windows 8 Pro (wersje 32- i 64-bitowe)
5. Windows 8.1 (32-bit, 64-bit)
6. Windows Server 2003 (32-bit, 64-bit, R2, SP1 lub nowszy)
7. Windows XP SP3
8. Mac OS
9. Mac OS X 10.5 lub nowszy (32-bit, 64-bit)
10. Mac OS X Server 10.5 lub 10.6 (32-bit, 64-bit)

Oprogramowanie antywirusowe przeznaczone do rozbudowy systemów wykorzystywanych w jednostkach organizacyjnych LP powinno spełniać następujące ogólne minimalne wymagania funkcjonalno użytkowe:

1. Zintegrowany system ochrony dla stacji roboczych i serwerów, posiadający następujące moduły funkcjonalne systemu:
   1.1. Ochrona w czasie rzeczywistym przed oprogramowaniem typu: wirusy, trojany, robaki, adware, spyware i inne potencjalnie złośliwe oprogramowanie poprzez wykrywanie, usuwanie i blokownie dla stacji roboczych i serwerów;
   1.2. Ochrona przed oprogramowaniem szpiegującym dla stacji roboczych,
   1.3. Desktop firewall dla stacji roboczych,
   1.4. Centralizacja zdarzeń (logów),
   1.5. Aktywnie skanowanie e-mail w poszukiwaniu szkodliwego oprogramowania i spamu zanim dotrze do skrzynek pocztowych.
   1.6. Wbudowany program ostrzegający użytkowników o możliwej zawartości strony internetowej wraz z możliwością blokowania dostępu do wybranych stron internetowych.
2. Przyrostowe aktualizacje z FTP, HTTP, UNC, zasobów lokalnych oraz mapowanych dysków.
3. Możliwości wznowienia ściągania sygnatur od miejsca jego przerwania.
4. Wzajemne uwierzytelnianie poszczególnych komponentów komunikujących się poprzez sieć wraz z bezpieczną komunikacją.
5. Możliwość pracy bez bezpośredniego połączenia z siecią Internet.
6. Możliwość aktualizacji komponentów systemu bez bezpośredniego przyłączenia do sieci Internet.
7. Centralne repozytorium (relacyjna baza danych) dla zdarzeń logowanych przez wszystkie moduły systemu ochrony.
8. Zbieranie zdarzeń logowanych we wszystkich modułach dostarczanego systemu ochrony na wszystkich chronionych węzłach (komputerach i serwerach) i składowanie ich w centralnym repozytorium będącym integralną częścią systemu.

9. Zbieranie zdarzeń musi obejmować wszystkie zdarzenia logowane przez moduły dostarczonego oprogramowania.
10. Mechanizm zbierania zdarzeń musi umożliwiać ograniczenie zbieranych zdarzeń na podstawie wybieranego przez administratora kryterium.
11. Podsystem zbierający zdarzenia musi zapewniać centralnie zarządzanie z pojedynczej konsoli dla wszystkich komponentów oprogramowania,
12. Ochrona antywirusowa na podstawie sygnatur i heurystyczna z możliwością wyłączenia.
13. Skanowanie antywirusowe w chwili dostępu (real time), na żądanie i według harmonogramu.
14. Skanowanie pamięci operacyjnej komputera na żądanie.
15. Skanowanie rejestru komputera na żądanie.
16. Skanowanie poczty, załączników oraz folderów dla klientów typu MS Outlook oraz typu IBM Lotus Notes.
17. Moduł antyspyware działający w trybie czasu rzeczywistego w tle.
18. Ochrona zabezpieczanych stacji roboczych za pomocą lokalnej ściany ogniowej typu Desktop Firewall.
19. Możliwość blokowania portów (funkcjonalność typu desktop firewall).
20. Praca ściany ogniowej w trybie nauki niewidocznym dla użytkownika.
21. Tworzenie reguł ściany ogniowej w zależności od rodzaju połączenia (sieć firmowa, sieć publiczna).
22. Zarządzanie z centralnej konsoli wszystkimi komponentami dostarczonego oprogramowania umożliwiające zarządzanie komputerami (węzłami) ze wspólną i spójną polityką dla dowolnie i elastycznie definiowanych grup komputerów.
23. Możliwość automatycznego zainstalowania nowych silników, poprawek typu service pack oraz hot-fix z serwera zarządzającego.
24. Możliwość tworzenia architektury rozproszonej umożliwiającej w celu zminimalizowania ruchu związanego z ściąganiem nowych szczepionek, instalacji nowych wersji oprogramowania, poprawek, etc. instalacji nowych komponentów z lokalnego repozytorium.
25. Możliwość ograniczenia opcji konfiguracyjnych oprogramowania dostępnych dla użytkowników lub ich zabezpieczenia hasłem.
26. Prawo do aktualizacji oprogramowania, baz sygnatur i poprawek.
27. Możliwość przedłużenia subskrypcji na kolejny okres wraz z aktualizacją oprogramowania do najnowszej dostępnej wersji.

Załącznik nr 1 - Opis przedmiotu zamówienia i elementów równoważności oprogramowania za pomocą cech funkcjonalno-użytkowych.

1. SymantecEndPoint Protection 14.0 STD lic Gov Band A firmy Symantec Corporation lub równoważne

Program z zaawansowaną ochroną przed zagrożeniami, zapewniający wysoki stopień ochrony notebooków, stacji roboczych i serwerów przed szkodliwym oprogramowaniem, który instaluje się na komputerach klienckich za pośrednictwem tylko jednego agenta. Kompleksowo chroni wszystkie komputery, zapewniając im zabezpieczenie przed wirusami i aplikacjami szpiegującymi. Program służący również jako firewall i stoi na straży połączenia sieciowego, monitorując wszystkie pobierane i wysyłane dane. Ponadto przy jego użyciu da się kontrolować i nadzorować działające w obrębie sieci aplikacje i urządzenia.

Najważniejsze cechy produktu:

1. Funkcja prewencyjnego skanowania w poszukiwaniu zagrożeń działająca bez wykorzystania sygnatur.
2. Mechanizmy zapory sieciowej opartej na regułach oraz funkcja blokowania luk w zabezpieczeniach.
3. Zintegrowany zakres technologii bezpieczeństwa w jednym agencie i centralnej konsoli zarządzania, z intuicyjnym interfejsem użytkownika i możliwością tworzenia graficznych raportów z poziomu przeglądarki internetowej.
4. Ochrona przed wirusami.
5. Ochrona przed programami typu „spyware”.
6. Zapobieganie włamaniom.
7. Mechanizmy kontroli urządzeń zewnętrznych.
8. Technologia reputacji typu Insight, która wykrywa i blokuje nowe zagrożenia.
9. Mechanizm, który monitoruje działanie aplikacji pod kątem podejrzanych operacji, pozwalający w czasie rzeczywistym blokować ściśle ukierunkowane zagrożenia i ataki "dnia zerowego".
10. System zapobiegania włamaniom (typu IPS), który blokuje ataki w warstwie sieci, zanim te zdążą wyrządzić szkody w komputerze.
11. Optymalizacja pod kątem wydajności w systemach wirtualnych. Rozwiązanie, które automatycznie identyfikuje maszyny wirtualne i zarządza nimi. Bezpośrednia integracja z interfejsem API VMware, umożliwiająca wyszukiwanie złośliwego oprogramowania w nieaktywnych obrazach VMware.
12. Zintegrowany antywirus, antyspyware, firewall który zapobiega włamaniom, a także steruje urządzeniem i kontrolą aplikacji.
13. Centralne zarządzanie bezpieczeństwem fizycznych i wirtualnych systemów typu Windows i Mac punktów końcowych.
14. Uaktualnienie do samodzielnego egzekwowania kontroli dostępu do sieci bez dodatkowego wdrażania oprogramowania.
15. Migracja ze starszych wersji programu.
16. Ocena wieku, występowania i bezpieczeństwo niemal każdego pliku programu w Internecie.
17. Moduł wykonujący niekrytyczne zadań w zakresie bezpieczeństwa, gdy komputer jest bezczynny.

Załącznik nr 1 - Opis przedmiotu zamówienia i elementów równoważności oprogramowania za pomocą cech funkcjonalno-użytkowych.

2. Kaspersky Endpoint Security for Business Select firmy Kaspersky Lab lub równoważne

Kaspersky Endpoint Security for Business - Select umożliwia ochronę komputerów, urządzeń mobilnych oraz serwerów plików. Posiada kilka warstw zabezpieczeń - ochronę opartą na sygnaturach, ochronę proaktywną oraz ochronę opartą na chmurze. Kaspersky Endpoint Security for Business - Select zapewnia wysokiej jakości ochronę przed szkodliwymi aplikacjami, wirusami oraz atakami sieciowymi. Administrator ma do dyspozycji konsolę zarządzającą (Kaspersky Security Center), która znacząco ułatwia zarządzanie wszystkimi komputerami w sieci. Dostosowanie ochrony do potrzeb danej firmy nie będzie stanowiło problemu. Za pomocą konsoli zarządzającej można również zarządzać aktualizacjami oraz monitorować bezpieczeństwo firmowych komputerów.

Najważniejsze cechy produktu:

1. Konsola zarządzająca
2. Częste aktualizacje
3. Urgent Detection System (UDS)
4. Kontrola systemu
5. Aktywne leczenie
6. Głębsze poziomy ochrony
7. Ochrona oparta na chmurze
8. Zapora sieciowa z funkcją HIPS (Host-based Intrusion Prevention System)
9. Blokowanie ataków sieciowych
10. Ochrona przed szkodliwym oprogramowaniem dla wieloplatformowych serwerów plików
11. Łatwe zarządzanie i elastyczne generowanie raportów
12. Obsługa wirtualizacji
13. Ochrona mobilna przed szkodliwym oprogramowaniem
14. Kontrola aplikacji dla urządzeń mobilnych
15. Szyfrowanie w urządzeniach mobilnych
16. Konteneryzacja urządzeń mobilnych
17. Funkcje mobilnej ochrony przed szkodliwym oprogramowaniem
18. Zarządzanie urządzeniami mobilnymi
19. Kontrola aplikacji
20. Dynamiczna Biała lista w kontroli aplikacji
21. Kontrola urządzeń
22. Kontrola sieci

Składniki produktu:

- Kaspersky Security Center (wraz z Zarządzaniem systemami i MDM)
- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac
- Kaspersky Anti-Virus for Linux File Server
- Kaspersky Anti-Virus for Windows Server Enterprise Edition
- Kaspersky Security for Mobile

Załącznik nr 1 - Opis przedmiotu zamówienia i elementów równoważności oprogramowania za pomocą cech funkcjonalno-użytkowych.

3. ESET Endpoint Antivirus Suite firmy ESET lub równoważne

Program antywirusowy, który zapewnia pełną i nieprzerwaną ochronę komputera od momentu jego uruchomienia. Pracując w tle sprawdza wszystkie uruchamiane, otwierane czy zapisywane zbiory. W razie wykrycia wirusa czy innego wrogiego programu, natychmiast blokuje jego działanie i automatycznie usuwa. Zawiera centralną administrację - ESET Remote Administrator.

Najważniejsze cechy produktu:

1. Skuteczny silnik skanujący
2. Antywirus
3. Antyspyware
4. Zaawansowana kontrola urządzeń
5. System zapobiegania włamaniom (HIPS)
6. Skanowanie komunikacji szyfrowanej
7. Zarządzanie z poziomu konsoli administracyjnej
8. Inteligentne aktualizacje
9. Szczegółowe raporty
10. Wsparcie dla CISCO NAC
11. Ochrona w czasie rzeczywistym
12. Skanowanie na żądanie
13. Skanowanie w czasie rzeczywistym
14. Wspierane platformy - Wspierane platformy obejmują w tej chwili Solaris™ 10, NetBSD® 4, FreeBSD® 5, 6 i 7, Linux® Kernel 2.2, 2.4 i 2.6 oraz Novell SUSE Enterprise.
15. Wsparcie dla procesorów wielordzeniowych.
16. Moduł Self Defense - Moduł autoochrony chroni Twój komputer przed wyłączeniem jego zabezpieczeń przez użytkownika lub przez zagrożenie internetowe.
17. Przywracanie wcześniejszej wersji bazy sygnatur wirusów lub modułów programu

4. ESET Endpoint Security Suite firmy ESET lub równoważne.

Kompletna ochrona stacji roboczych oraz serwerów plikowych w firmie. Łączy bezkonkurencyjną ochronę antywirusową i antyspyware programu ESET Endpoint ze skutecznym firewallem, filtrem antyspamowym oraz kontrolą dostępu do stron WWW.

Najważniejsze cechy produktu:

1. Antywirus
2. Antyspyware
3. Zapora osobista (firewall)
4. Antyspam
5. System zapobiegania włamaniom HIPS
6. Kontrola treści. Funkcjonalność ta pozwala zarządzać dostępem do stron www w zależności od kategorii w jakiej znajduje się dana strona. Administrator ma do dyspozycji ponad 140 różnych kategorii stron internetowych. Kategorie są na bieżąco uzupełniane o najczęściej odwiedzane Polskie witryny. Polityki filtrowania stron

mogą być przydzielane pojedynczym użytkownikom jak i całym grupom użytkowników.

7. Kontrola urządzeń peryferyjnych. Funkcjonalność ta umożliwia administratorowi zdefiniowanie typów urządzeń, które mogą być wykorzystywane na stacjach klienckich. Możemy zablokować: dyski zewnętrzne, płyty CD i DVD, pendrive'y, urządzenia komunikacyjne na USB (w tym modemy), drukarki USB, urządzenia połączone przez Firewire lub Bluetooth itd. Istnieje również możliwość ustalenia białej listy określonych nośników wymiennych w oparciu o ich producenta, model czy nawet numer seryjny; opcje dostępu obejmują jego całkowite blokowanie, możliwość samego odczytu oraz odczytu i zapisu.
8. Optymalizacja skanowania oparta o tzw. białe listy „bezpiecznych" plików, połączona z bazą reputacji plików umieszczoną w chmurze. ESET Live Grid rozpoznaje pliki na twardym dysku użytkownika i sprawdza ich reputację na serwerach producenta
9. Instalacja modułowa umożliwia Administratorowi funkcję instalowania niektórych komponentów programu (np. firewalla, ochrony klienta pocztowego)
10. Skanowanie komunikacji szyfrowanej - zawartość szyfrowanych protokołów HTTPS i POP3S oraz pliki skompresowane są dokładnie skanowane pod kątem obecności zagrożeń.
11. Zintegrowane narzędzie do analizy systemu operacyjnego typu SysInspector.
12. Tworzenie ratunkowego dysku bootowalnego narzędziem SysRescue
13. Moduł autoochrony uniemożliwiający wyłączenie zabezpieczeń programu przez użytkownika lub przez zagrożenie internetowe (SelfDefense)
14. Ochrona serwerów plikowych Windows – automatyczne wykluczenia, inteligentne aktualizacje, szczegółowe raporty, wsparcie dla Cisco NAC, ochrona w czasie rzeczywistym (on-access), skanowanie na żądanie (on-demand)
15. Ochrona serwerów plikowych Linux/BSD/Solaris – skanowanie na żądanie (on-demand), skanowanie w czasie rzeczywistym (on-access), zadania predefiniowane, współpraca z konsolą Remote Administrator, konfiguracja dostosowana do użytkownika, interfejs dostępny z poziomu przeglądarki internetowej, inteligentny skaner, moduł Daemon, wsparcie dla procesorów wielordzeniowych

5. ESET Endpoint Security dla systemów Android firmy ESET lub równoważne.

ESET Endpoint Security dla systemów Android to proaktywna i wszechstronna ochrona przed wirusami, spyware, adware, trojanami, robakami, rootkitami i innym szkodliwym oprogramowaniem. Dzięki zastosowaniu zaawansowanej heurystyki ESET Mobile Security chroni urządzenia nawet pomiędzy aktualizacją bazy sygnatur. Zastosowanie szybkiego silnika pozwala łatwo porządkować skrzynkę odbiorczą poprzez filtrowanie wiadomości SMS oraz MMS od nieznanych lub niechcianych nadawców.

Najważniejsze cechy produktu:

1. Pakiet bezpieczeństwa dla urządzeń mobilnych.
   Urządzenia mobilne mają szerokie zastosowanie w komunikacji, rozrywce i biznesie. Coraz więcej osobistych i zastrzeżonych informacji jest przechowywanych na tego typu urządzeniach. Wraz ze wzrostem popularności, oraz przez zastosowanie coraz bardziej wyszukanych funkcji (min. bezprzewodowej komunikacji), urządzenia mobilne stają się celem ataków.

2. Ochrona Anti-Theft.
   Ochrona przed kradzieżą danych realizowana jest poprzez autoryzację karty SIM jako zaufanej. Jeżeli użyta zostanie niezaufana karta SIM urządzenie automatycznie wyśle na wskazany wcześniej numer telefonu wiadomość zawierającą numer aktualnej karty SIM, numer IMSI oraz numer IMEI telefonu. Dodatkowo jest możliwość zdalnego skasowania wszystkich danych zapisanych na urządzeniu i kartach pamięci podłączonych do urządzenia poprzez wysłanie wiadomości SMS z wcześniej zdefiniowanym przez użytkownika hasłem.
3. Audyt urządzenia mobilnego.
   Opcja audytu urządzenia pozwala na sprawdzenie wszystkich procesów uruchomionych na urządzeniu, a także sprawdzenie statusu wykorzystania baterii, aktywności bluetooth, IR a także wolnego miejsca na dysku urządzenia. Z poziomu oprogramowania można włączyć lub wyłączyć wybrane funkcje w celu uzyskania optymalnej konfiguracji ustawień urządzenia.
4. Niskie obciążenie urządzenia.
   ESET Mobile Security charakteryzuje się niskim zużyciem procesora i pamięci oraz kompaktowymi aktualizacjami, które minimalizują wielkość koniecznej transmisji danych. Zabezpieczenie załączników do wiadomości e-mail oraz innych otwieranych i transmitowanych danych nie obniża szybkości działania urządzenia.