Zał. Nr 1

Opis przedmiotu zamówienia.

Przedmiotem zamówienia jest zakup licencji na oprogramowanie antywirusowe oraz Licencji Cal (licencje dostępowe) dla usługi Active Directory dla jednostek organizacyjnych gmin: Moszczenica, Ujazd, Będków i Czarnocin w ramach realizacji projektu „E-Leader szansą na przeciwdziałanie wykluczeniu cyfrowemu dla mieszkańców gmin: Moszczenica, Ujazd, Będków i Czarnocin"

A – Część I zamówienia:

Dostawa oprogramowania antywirusowego dla jednostek organizacyjnych gmin: Moszczenica, Ujazd, Będków i Czarnocin w ramach realizacji projektu „E-Leader szansą na przeciwdziałanie wykluczeniu cyfrowemu dla mieszkańców gmin: Moszczenica, Ujazd, Będków i Czarnocin".
Wykonawca zobowiązany jest do doboru licencji oprogramowania (np. licencja edukacyjna) do typu placówki (placówki szkolne biblioteki, urzędy gmin).
Jednostki dla, których należy dostarczyć oprogramowanie antywirusowe:
- **12 placówek szkolnych – łącznie ok. 360 stanowisk** (w tym: 7 szkół w Gminie Moszczenica, 2 szkoły w Gminie Czarnocin, 1 szkoła w Gminie Będków, 2 szkoły w Gminie Ujazd) - oferta powinna obejmować dla tych komputerów licencje dedykowane dla jednostek edukacyjnych o ile producent takie posiada;
- **48 licencji** na stanowiska znajdujące się w Urzędzie Gminy w Moszczenicy

Okres obowiązywania subskrypcji na oprogramowanie wynosi 3 lata.

Wymagania dla oprogramowania:
Wykonawca jest zobowiązany dostarczyć wraz z licencjami na stanowiska końcowe konsolę administracyjną, za pomocą, której można kontrolować wszystkie dostarczone przez Wykonawcę technologie zarządzania bezpieczeństwem i systemami zainstalowanymi na komputerach. Zamawiający informuje, że wszystkie komputery, które są objęte niniejszym zamówieniem znajdują się w 4 drzewach Active Directory. Dostarczone oprogramowanie monitorujące stacje musi gwarantować wgląd w każdy punkt końcowy i każde urządzenie w sieci, na którym zainstalowano oprogramowanie antywirusowe.

Dostarczone powinno spełniać następujące wymagania:

1. Program musi wspierać następujące platformy:
   - Microsoft Windows 8 Professional / Enterprise;
   - Microsoft Windows 8 Professional / Enterprise x64 Edition;
   - Microsoft Windows 7 Professional / Enterprise / Ultimate SP0 lub wyższy;
   - Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP0 lub wyższy;
   - Microsoft Windows Vista Business / Enterprise / Ultimate SP2;
   - Microsoft Windows Vista Business / Enterprise / Ultimate x64 Edition SP2;
   - Microsoft Windows XP Professional SP3 lub wyższy.
2. Program musi posiadać polskojęzyczny interfejs konsoli programu i jego monitora na stacjach roboczych.
3. Program powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.
4. Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony.
5. Program musi mieć możliwość skanowania i klasyfikowania plików oraz odsyłaczy do zasobów sieciowych na podstawie informacji gromadzonych w oparciu o dane dostarczane przez producenta.
6. Program musi mieć możliwość wyświetlenia podsumowania o aktywności, reputacji i lukach w aplikacjach aktualnie uruchomionych w systemie.
7. Program musi mieć możliwość monitorowania prób uruchamiania aplikacji przez użytkowników zgodnie z określonymi regułami.
8. Program musi mieć możliwość klasyfikacji wszystkich aplikacji i możliwość ograniczenia ich działania na podstawie ich stanu.

9. Program musi posiadać dedykowany moduł blokujący określone kategorie urządzeń (np. pamięci masowe, urządzenia Bluetooth itp.).

   - Możliwość tworzenia reguł blokujących/zezwalających na korzytanie z danego urządzenia w zależności od konta, na którym pracuje użytkownik, określenia przedziału czasu, w którym użytkownik będzie miał możliwość tylko zapisu bądź tylko odczytu, ewentualnie zapisu i odczytu.

   -Możliwość blokowania urządzeń według ich rodzaju: dyski, USB, drukarki itp. w zależności od czasu, konta użytkownika systemu Windows oraz rodzaju operacji: odczyt/zapis.

   - Możliwość utworzenia listy zaufanych urządzeń na podstawie modelu, bądź identyfikatora urządzenia dla określonego konta użytkownika systemu Windows.

10. Użytkownik musi mieć możliwość wysłania do administratora zgłoszenia z prośbą o umożliwienie dostępu do zablokowanego urządzenia; nośnik wymienny, napęd CD-ROM itd.
11. Użytkownik musi mieć możliwość wysłania do administratora zgłoszenia z prośbą o umożliwienie dostępu do zablokowanego zasobu sieciowego.
12. Użytkownik musi mieć możliwość wysłania do administratora zgłoszenia z prośbą o umożliwienie dostępu do zablokowanej aplikacji.
13. Kontrola sieci – kontrola dostępu do zasobów sieciowych w zależności od ich zawartości i lokalizacji:

    - Możliwość definiowania reguł filtrujących zawartość na wybranej stronie lub wszystkich stronach w zależności od kategorii zawartości: pornogafia, narkotyki, broń, gry, sieci społecznościowe, banery, itd.

    - Możliwość definiowania reguł blokujących bądź zezwalających na wyświetlanie określonej treści na wybranej stronie lub wszystkich stronach w zależności od kategorii danych: pliki wideo, audio, archiwa itd.

14. Monitor wykrywania luk w aplikacjach zainstalowanych na stacji roboczej oraz w samym systemie operacyjnym.
15. Ochrona przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem (w tym Java i ActiveX).
16. Możliwość wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich.
17. Wbudowany moduł skanujący protokoły POP3, SMTP, IMAP i NNTP niezależnie od klienta pocztowego.
18. Skaner poczty powinien mieć możliwość zmiany nazwy lub usuwania określonych typów załączników.
19. Wbudowany moduł skanujący ruch HTTP w czasie rzeczywistym niezależnie od przeglądarki.
20. Wbudowany moduł skanujący ruch komunikatorów ICQ, MSN, AIM, Yahoo!, Jabber, Google Talk, Mail.Ru Agent oraz IRC.
21. Wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa.
22. Wbudowany moduł chroniący przed phishingiem.
23. Moduł zapory ogniowej z możliwością:

    - Tworzenia reguł monitorowania aktywności sieciowej dla wszystkich zainstalowanych aplikacji, w oparciu o charakterystyki pakietów sieciowych i podpis cyfrowy aplikacji.

    - Tworzenia nowych zestawów warunków i działań wykonywanych na pakietach sieciowych oraz strumieniach danych dla określonych protokołów, portów i adresów IP.

    - Zdefiniowania zaufanych podsieci, dla których nie będą stosowane żadne reguły zapory.

24. Ochrona przed niebezpiecznymi rodzajami aktywności sieciowej i atakami, możliwość tworzenia reguł wykluczających dla określonych adresów/zakresów IP.
25. Kontrola systemu poprzez ochronę proaktywną przed nowymi zagrożeniami, które nie znajdują się

w antywirusowych bazach danych:

- Kontrola aktywności aplikacji, dostarczanie szczegółowych informacji dla innych modułów aplikacji w celu zapewnienia jeszcze bardziej efektywnej ochrony.

- Możliwość wycofywania zmian wprowadzanych w systemie przez szkodliwe oprogramowanie nawet w poprzednich sesjach logowania.

26. Centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym.
27. Leczenie i usuwanie plików z archiwów następujących formatów RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.
28. Możliwość zablokowania dostępu do ustawień programu dla użytkowników nie posiadających uprawnień administracyjnych.
29. Terminarz pozwalający na planowanie zadań, w tym także terminów automatycznej aktualizacji baz sygnatur.
30. Możliwość wysłania podejrzanego obiektu do producenta oprogramowania antywirusowego w celu analizy.
31. Monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
32. Możliwość tworzenia list zaufanych procesów, dla których nie będzie monitorowana aktywność plikowa, aktywność aplikacji, nie bądą dziedziczone ograniczenia nadrzędnego procesu, nie będzie monitorowana aktywność aplikacji potomnych, dostęp do rejestru oraz ruch sieciowy.
33. Możliwość dynamicznej zmiany użycia zasobów systemowych w zależności od obciążenia systemu przez aplikacje użytkownika.
34. Program posiada funkcję chroniącą pliki, foldery i klucze rejestru wykorzystywane przez program przed zapisem i modyfikacją.
35. Program posiada możliwość wyłączenia zewnętrznej kontroli usługi antywirusowej.
36. Program posiada możliwość zresetowania wszystkich ustawień włącznie z regułami stworzonymi przez użytkownika.
37. Program ma możliwość zdefiniowania portów, które będą monitorowane lub wykluczone z monitorowania przez moduły skanujące ruch sieciowy (z wyłączeniem zapory ogniowej).
38. Skanowanie w czasie rzeczywistym:

    - Uruchamianych, otwieranych, kopiowanych, przenoszonych lub tworzonych plików.

    - Pobieranej z Internetu poczty elektronicznej (wraz z załącznikami) po protokołach POP3, SMTP, IMAP i NNTP niezależnie od klienta pocztowego.

    - Plików pobieranych z Internetu po protokole HTTP.

    - Poczty elektronicznej przetwarzanej przez program MS Outlook niezależnie od wykorzystywanego protokołu pocztowego.

    - Treści i plików przesyłanych z wykorzystaniem komunikatorów ICQ, MSN, AIM, Yahoo!, Jabber, Google Talk, Mail.Ru Agent oraz IRC.

39. W przypadku wykrycia wirusa monitor antywirusowy może automatycznie:

    - Podejmować zalecane działanie czyli próbować leczyć, a jeżeli nie jest to możliwe usuwać obiekt

    - Rejestrować w pliku raportu informację o wykryciu wirusa

    - Powiadamiać administratora przy użyciu poczty elektronicznej lub poleceniem NET SEND

    - Utworzyć kopie zapasową przed podjęciem próby leczenia lub usunięcia zainfekowanego pliku

    - Poddać kwarantannie podejrzany obiekt

40. Skaner antywirusowy może być uruchamiany automatycznie zgodnie z terminarzem; skanowane są wszystkie lokalne dyski twarde komputera.
41. Informowanie o wykryciu podejrzanych działań uruchamianych aplikacji (np. modyfikacje rejestru, wtargnięcie do innych procesów) wraz z możliwością zezwolenia lub zablokowania takiego



działania.

42. System antywirusowy posiada możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia.
43. Program musi posiadać możliwość skanowania obiektów poddanych kwarantannie po zakończonej aktualizacji.
44. Program musi posiadać możliwość cofnięcia ostatniej aktualizacji w przypadku uszkodzenia zestawu uaktualnień.
45. Program musi posiadać możliwość określenia ustawień serwera proxy w przypadku, gdy jest on wymagany do nawiązania połączenia z Internetem.
46. Program powinien posiadać możliwość raportowania zdarzeń informacyjnych.
47. Program powinien posiadać możliwość określenia okresu przechowywania raportów.
48. Program powinien posiadać możliwość określenia okresu przechowywania obiektów znajdujących się w magazynie kopii zapasowych oraz kwarantannie.
49. Program musi posiadać możliwość wyłączenia zaplanowanych zadań skanowania podczas pracy na bateriach.
50. Program musi posiadać możliwość wyeksportowania bieżącej konfiguracji programu w celu jej późniejszego zaimportowania na tym samym lub innym komputerze.
51. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
52. Program musi mieć możliwość włączenia opcji współdzielenia zasobów z innymi apikacjami.

B – Część II zamówienia:

Dostawa następujących licencji Cal – licencji dostępowych:

1) **Licencje dla Ostatecznych Beneficjentów**
   Nazwa: WinSvrExtConn 2012 OLP NL Gov,
   Ilość: 2 licencje

2) **Licencje dla szkół**
   Nazwa licencji: Windows® Server CAL Single License/Software Assurance Pack Academic OPEN No Level Device CAL R18-00200 Non-specific,
   Ilość : **178 licencji** (105 licencji dla szkół w Gminie Moszczenica, 13 licencji dla szkół w Gminie Czarnocin, 40 licencji dla szkoły w Gminie Będków, 20 licencji dla szkół w Gminie Ujazd)

3) **licencje CAL dla komputerów w 4 Urzędach Gmin**
   Nazwa: WinSvrCAL LicSAPk OLP NL Gov DvcCAL, R18-01634
   Ilość: **95 licencji** (28 licencji dla Gminy Moszczenica, 25 licencji dla Gminy Będków, 20 licencji dla Gminy Ujazd, 22 licencji dla Gminy Czarnocin)

4) **licencje na pocztę dla Urzędów Gmin**
   Nazwa licencji: ExchgStdCAL LicSAPk OLP NL Gov UsrCAL, 381-02592
   Ilość: **34 licencji** (28 licencji dla Urzędu Gminy Moszczenica, 3 licencje dla Urzędu Gminy Będków, 3 licencje dla Urzędu Gminy Ujazd)

5) **licencje na pocztę dla szkół**
   Nazwa licencji: ExchgStdCAL LicSAPk OLP NL Academic
   Ilość: 157 licencji (150 licencji dla Gminy Moszczenica, 5 licencji dla Gminy Będków, 2 licencje dla Gminy Ujazd)

