Fundusze Europejskie Program Regionalny | Rzeczpospolita Polska | Mazowsze. serce Polski | Unia Europejska Europejskie Fundusze Strukturalne i Inwestycyjne

Wydatek współfinansowany z Europejskiego Funduszu Społecznego

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa licencji na oprogramowanie antywirusowe wraz z centralnym zarządzaniem. Licencja musi spełniać określone warunki:

1. Licencja na 600 stanowisk komputerowych, w tym 15 instalacji serwerowych (ilekroć w SOPZ mowa jest o licencji należy przez to rozumieć także sublicencję).
2. Licencja ma obowiązywać od dnia 6 maja 2019 r., przez okres 36 kolejnych miesięcy od dnia zawarcia umowy.
3. W zakresie autorskich praw majątkowych na podstawie dostarczonej licencji Zamawiający musi mieć prawo korzystania z oprogramowania antywirusowego wraz z centralnym zarządzaniem, którego dotyczy licencja, na następujących polach eksploatacji: trwałe lub czasowe zwielokrotnianie oprogramowania w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie, w tym jego zwielokrotnianie dokonywane podczas wprowadzania, wyświetlania, stosowania, przekazywania lub jego przechowywania, i zwielokrotnianie oprogramowania dowolną techniką, w tym techniką zapisu magnetycznego lub techniką cyfrową, w szczególności w systemach informatycznych Zamawiającego.
4. Licencja w okresie jej obowiązywania musi umożliwiać Zamawiającemu:
   a) korzystanie z oprogramowania w ramach wszystkich funkcjonalności w dowolny sposób w zakupionej liczbie,
   b) instalowanie i deinstalowanie oprogramowania pod warunkiem zachowania liczby udzielonych licencji;
   c) sporządzanie kopii zapasowych (kopii bezpieczeństwa) nośników instalacyjnych i nośników z zainstalowanym oprogramowaniem;
   d) korzystanie z produktów powstałych w wyniku eksploatacji oprogramowania przez Zamawiającego, w szczególności danych, raportów, zestawień oraz innych dokumentów kreowanych w ramach tej eksploatacji oraz modyfikowania tych produktów i dalszego z nich korzystania;
   e) aktualizację oprogramowania wydawanego przez jego producenta, jak również aktualizację bazy wirusów.

Obecne oprogramowanie:

Zamawiający w chwili obecnej posiada oprogramowanie antywirusowe ESET Endpoint Antivirus Suite wraz z centralnym zarządzaniem Licencje na 600 stanowisk (w tym 15 instalacji serwerowych).

W przypadku wyboru oferty na posiadane już oprogramowanie antywirusowe ESET Endpoint Antivirus Suite wraz z centralnym zarządzaniem ,nr posiadanej przez Zamawiającego licencji zostanie przekazany w momencie podpisania Umowy z Wykonawcą.

Oprogramowanie musi posiadać:

1. Pełne wsparcie dla system Windows 7 Professional/Windows 8 Professional/Windows 8.1 Professional, Windows 10 Professional.
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dla stacji roboczych Windows dostępna w języku polskim.
4. Pomoc w programie (help) i dokumentacja do programu w języku polskim.

Ochrona antywirusowa:

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych programów: adware, spyware, scareware, phishing, hacktools itp.
3. Ochrona przed rootkitami wykrywająca aktywne i nieaktywne rootkity.

4. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
5. Możliwość wykluczenia ze skanowania skanera dostępowego: napędów, katalogów, plików lub procesów.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików na żądanie lub według harmonogramu.
7. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np. co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
8. Skanowanie na żądanie pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. Technologia zapobiegająca powtórnemu skanowaniu sprawdzonych już plików, przy czym maksymalny czas od ostatniego sprawdzenia pliku nie może być dłuższy niż 4 tygodnie, niezależnie od tego czy plik był modyfikowany czy nie.
10. Możliwość określania poziomu obciążenia procesora podczas skanowania na żądanie i według harmonogramu.
11. Możliwość skanowania dysków sieciowych i dysków przenośnych.
12. Rozpoznawanie i skanowanie wszystkich znanych formatów kompresji.
13. Możliwość definiowania listy procesów, plików, folderów i napędów pomijanych przez skaner dostępowy.
14. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli.
15. Dodatek do aplikacji MS Outlook umożliwiający podejmowanie działań związanych z ochroną z poziomu programu pocztowego.
16. Skanowanie i oczyszczanie poczty przychodzącej POP3 w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
17. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
18. Możliwość definiowania różnych portów dla POP3, SMTP i IMAP na których ma odbywać się skanowanie.
19. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
20. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
21. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
22. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
23. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe.
24. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.
25. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
26. Możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.
27. Aktualizacja dostępna z bezpośrednio Internetu lub offline – z pliku pobranego zewnętrznie.
28. Możliwość samodzielnej aktualizacji sygnatur wirusów ze stacji roboczej (np. komputery mobilne).
29. Możliwość ukrycia programu na stacji roboczej przed użytkownikiem.
30. Kontrola zachowania aplikacji do wykrywania podejrzanie zachowujących się aplikacji.
31. Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu.

Zdalne administrowanie ochroną:

1. Pełna integracja z Active Directory – import kont komputerów i jednostek organizacyjnych.
2. Opcja automatycznej instalacji oprogramowania klienckiego na wszystkich podłączonych komputerach Active Directory.

3. Możliwość uruchomienia serwera centralnej administracji i konsoli zarządzającej na stacjach Windows 7 Professional/ Windows 8 Professional/ Windows 8.1 Professional, Windows 10 Professional oraz na serwerach 2008/2008R2/2012 – 32- i 64- bitowe systemy.
4. Centralna instalacja oprogramowania na końcówkach (stacjach roboczych) z systemami operacyjnymi Windows 7 Professional/ Windows 8 Professional/ Windows 8.1 Professional, Windows 10 Professional.
5. Centralne zarządzanie programami służącymi do ochrony stacji roboczych Windows.
6. Do instalacji zdalnej i zarządzania zdalnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy.
7. Możliwość zarządzania ochroną urządzeń mobilnych z poziomu konsoli (przynajmniej aktualizacje, ochronę przeglądarek, skanowania zasobów, synchronizacji raportów).
8. Możliwość kontekstowego zastosowania ustawień danej stacji dla całej grupy.
9. Możliwość eksportu/importu ustawień dla stacji/grupy stacji.
10. Możliwość zarządzania różnymi wersjami licencyjnymi oprogramowania producenta z jednego okna konsoli.
11. Możliwość zainstalowania zapasowego serwera zarządzającego, przejmującego automatycznie funkcje serwera głównego w przypadku awarii lub odłączenia serwera głównego.
12. Możliwość zdalnego zarządzania serwerem centralnego zarządzania przez przeglądarki internetowe (z sieci lokalnej i spoza niej).
13. Szyfrowanie komunikacji między serwerem zarządzającym a klientami.
14. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
15. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania).
16. Możliwość sprawdzenia z centralnej konsoli zarządzającej zainstalowanych na stacjach/serwerach oprogramowania (tj. nazwa, wersja, producent, data instalacji).
17. Możliwość stworzenia białej i czarnej listy oprogramowania, i późniejsze filtrowanie w poszukiwaniu stacji je posiadających.
18. Odczyt informacji o zasobach stacji (procesor i jego taktowanie, ilość pamięci RAM i ilość miejsca na dysku.
19. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
20. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.
21. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.
22. Możliwość zmiany konfiguracji na stacjach i serwerach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).
23. Możliwość przeglądania statystyk ochrony antywirusowej w postaci tekstu lub wykresów.
24. Możliwość przesłania komunikatu, który wyświetli się na ekranie wybranej stacji roboczej lub grupie stacji roboczych.
25. Komunikat można wysłać do wszystkich lub tylko wskazanego użytkownika stacji roboczej.
26. Możliwość zminimalizowania obciążenia serwera poprzez ograniczenie ilości jednoczesnych procesów synchronizacji, aktualizacji i przesyłania plików do stacji roboczych.
27. Dostęp do kwarantanny klienta ma być z poziomu systemu centralnego zarządzania.

Wymagania dodatkowe

W przypadku wyboru przez Zamawiającego oferty na obecnie posiadane oprogramowanie, Wykonawca zobowiązany jest w cenie dostawy licencji:

- do instalacji lub uaktualnienia serwera i konsoli zarządzania do najnowszej wydanej wersji;
- aktualizacji lub jeśli to konieczne odinstalowania obecnej i zainstalowania najnowszej wersji oprogramowania antywirusowego na stacjach klienckich.

Natomiast gdy Zamawiający wybierze ofertę na oprogramowanie antywirusowe innego producenta niż dotychczas, Wykonawca w cenie dostawy licencji zobowiązuje się do:

- instalacja serwera i konsoli zarządzania;
- odinstalowanie istniejących instancji oprogramowania ESET Endpoint Antivirus Suite na stacjach klienckich;
- instalacji nowego oprogramowania antywirusowego na stacjach klienckich.

Zarówno w przypadku aktualizacji obecnego oprogramowania jak i przy wdrożeniu nowego oprogramowania Wykonawca zobowiązuje się do przeszkolenie personelu technicznego (dwóch osób) w zakresie używania, zarządzania oraz administrowania programem, konsolą zarządzania (np. instalacja zdalna agentów, monitorowanie bieżącej bazy komputerów, uaktualnień) w cenie dostawy licencji nie później niż w ciągu pięciu dni od dnia aktualizacji/wdrożenia oprogramowania. Ostateczny termin szkolenia będzie zależał od oferty wykonawcy ponieważ stanowi jedno z kryteriów oceny ofert.