Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego na podstawie art. 275 pkt. 1 ustawy Pzp **na przedłużenie licencji na oprogramowanie do ochrony antywirusowej.**
Nr sprawy TP-89/23/DW

Opis przedmiotu zamówienia (OPZ)

Zamawiający użytkuje następujące rozwiązanie w zakresie podstawowego oprogramowania do ochrony antywirusowej:
- 1600 licencji ochrony komputerów użytkowników (WithSecure Elements / F-Secure Protection Service for Business Computer Protection)
- 30 licencji ochrony serwerów (WithSecure Elements / F-Secure Protection Service for Business Server Protection)
- 750 licencji (WithSecure Elements / F-Secure F-Secure Email and Server Security

Przedmiotem zamówienia jest dostawa przedłużenia licencji na oprogramowanie do ochrony system antywirusowej. Wszystkie licencje, które będą dostarczone w ramach realizacji przedmiotu zamówienia będą obowiązywać przez okres 24 miesięcy liczony od dnia aktywacji dostarczonych licencji.

Szczegółowy zakres przedłużenia licencji na oprogramowanie do ochrony antywirusowej:
- 1800 licencji ochrony komputerów użytkowników,
- 30 licencji ochrony serwerów,
- 24 miesiące ochrony licząc od dnia aktywacji licencji na oprogramowanie do ochrony antywirusowej,
- rozwiązanie objęte centralną konsolą zarządzania dostępną z chmury,
- dostępne wsparcie techniczne,
- czas realizacji 14 dni od daty podpisania umowy.

Szczegółowe wymagania rozwiązania oprogramowania do ochrony antywirusowej, w tym minimalne techniczne, funkcjonalne i użytkowe wymagania Zamawiającego dla rozwiązania równoważnego:

Dział I. Licencja i wymagania ogólne
1. Licencja / licencje przeznaczona dla firm. Umożliwiająca użytkowanie rozwiązania na 30 serwerach i 1800 komputerach użytkowników.
2. Możliwość zwiększenia liczby licencji w przyszłości.
3. Dostarczenie w pełni funkcjonującego rozwiązania, umożliwiającego pełne wdrożenie wszystkich wymaganych funkcjonalności.

Dział II. Oprogramowanie musi zapewniać:
1. Ochrona antywirusowa komputerów z systemami operacyjnymi: Microsoft Windows 7 z dodatkiem SP1, Microsoft Windows 8.1 (32-bit i 64-bit), Microsoft Windows 10, Microsoft Windows 11, MacOS 11 “Big Sur”, MacOS 10.15 “Catalina”, MacOS 10.14 “Mojave”,
2. Ochrona antywirusowa serwerów z serwerowymi systemami operacyjnymi: Microsoft® Windows Server 2008 R2, Microsoft® Windows Server 2012, Microsoft® Windows Server 2016, • Microsoft® Windows Server 2019, Microsoft® Windows Server 2022.

Dział III. Ochrona antywirusowa i antyspyware:
1. Rozwiązanie ocenione pozytywnie przez niezależne laboratorium (zajmujące się bezpieczeństwem informatycznym) i/lub czasopisma komputerowe (zajmujące się bezpieczeństwem informatycznym)
2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami o podobnym charakterze zwyczajowo wchodzących w skład ochrony antywirusowej/ochrony spyware,
3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hackerskich, backdoor, itp,
4. Wbudowana technologia do ochrony przed rootkitami,
5. Skanowanie w czasie rzeczywistym otwieranych, pobieranych, zapisywanych i wykonywanych plików,

6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie” lub według harmonogramu,
7. Możliwość skanowania dysków przenośnych,
8. Skanowanie plików spakowanych i skompresowanych,
9. Możliwość umieszczenia na liście wyłączenia ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach,
10. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy popularnych klientów poczty e-mail: MS Outlook, Outlook Express, Windows Live Mail, Eudora, Mozilla Thunderbird
11. Skanowanie i oczyszczanie poczty przychodzącej z użyciem protokołów: POP/POP3S3 i IMAP/IMAPS „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego),
12. Automatyczna działanie skanera antywirusowego w zakresie ruchu POP3 i IMAP dowolnego klienta pocztowego bez konieczności zmian w konfiguracji oprogramowania pocztowego,
13. Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie,
14. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu zainfekowanych wiadomości e-mail,
15. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie. Informacja o wykryciu zainfekowanego ruchu ma być również dostępna dla administratorów IT rozwiązania,
16. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie,
17. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS, (wszystkie) z uwzględnieniem różnych wariantami szyfrowania (SSL, TLS, itd.),
18. Prawidłowa współpraca oprogramowania antywirusowego w zakresie odbioru/wysyłki poczty e-mail na serwery oparte o system operacyjny Linux i szyfrowanie transmisji poczty TLS,
19. Prawidłowa współpraca oprogramowania antywirusowego w zakresie odbioru/wysyłki poczty e-mail na serwery oparte o rozwiązanie MS Exchange.
20. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe, itd.
21. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego,
22. Możliwość zabezpieczenia konfiguracji programu antywirusowego hasłem, w taki sposób, aby użytkownik pracujący na komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła,
23. Możliwość zabezpieczenia programu przed odinstalowaniem przez niepowołane osoby, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie odinstalowania program musi pytać o hasło,
24. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji - poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji,
25. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD, czytników kart,
26. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia,
27. W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika,
28. Automatyczna, aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. Nowe uaktualnienie dostępne co najmniej raz dziennie.
29. Program antywirusowy ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów.
30. Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu lub bezpośrednio przez producenta. Możliwość kontaktu e-mail i telefonicznego w języku polskim. Dostępność pomocy technicznej w dni powszednie: poniedziałek – piątek w godz. 8:00 – 16:00.
31. Rozwiązanie posiada polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na komputerach użytkowników oraz serwerach.

32. Agent instalowany na stacjach końcowych i serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.
33. Agent instalowany na stacjach końcowych i serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.
34. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach.
35. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do chmury, w celu wykrywania niebezpiecznych zdarzeń.
36. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w chmurze a nie na monitorowanej stacji końcowej.
37. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do chmury, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.
38. Maksymalna ilość wysyłanych danych do chmury przez agenta uruchomionego na stacji roboczej z systemami Windows nie przekracza 50 MB w ciągu doby.
39. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z chmurą, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
40. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
41. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do chmury, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.
42. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.

Dział IV. Centralne zarządzanie:

1. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową.
2. Komunikacja miedzy konsolą centralnego zarządzania a stacjami klienckimi, powinna być realizowana w sposób bezpieczny (zabezpieczona hasłem lub/i korzystać z połączenia szyfrowanego).
3. Możliwość uruchomienia centralnego skanowania wybranych (lub wszystkich) stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania (go) do konsoli zarządzającej.
4. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych).
5. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego.
6. Funkcjonalność centralnej aktualizacji oprogramowania antywirusowego na serwerach i komputerach użytkowników.
7. Możliwość zmiany konfiguracji na stacjach roboczych z centralnej konsoli zarządzającej lub lokalnie.
8. Centralna konsola zarządzająca ma być wyposażona w wygodny mechanizm zarządzania licencjami, który umożliwi sumowanie liczby licencji nabytych przez Zamawiającego. Dodatkowo konsola ma stale nadzorować, ile licencji spośród puli nie zostało jeszcze wykorzystanych. Konsola informuje o przekroczeniu liczby posiadanych licencji.
9. Dostęp do kwarantanny klienta ma być z poziomu konsoli centralnego zarządzania.
10. Możliwość przywrócenia (na) lub pobrania zainfekowanego pliku ze stacji klienckiej przy wykorzystaniu centralnej konsoli zarządzania.
11. Konsola centralnego zarządzania ma być wyposażona w mechanizm informowania administratora o wykryciu nieprawidłowości w funkcjonowaniu oprogramowania antywirusowego zainstalowanego na serwerach i komputerach użytkowników, w tym przynajmniej informowaniu o: wygaśnięciu licencji na oprogramowanie antywirusowe, o nieaktywnej ochronie antywirusowej na stacji roboczej, starej wersji bazy o wirusach.
12. Informacja o wszystkich działania administrator-a/ów w centralnej konsoli zarządzania mają być zapisywane w logach.

Dział V. Wymagania dodatkowe

W przypadku zaoferowania oprogramowania do ochrony antywirusowej innego niż oprogramowanie, które obecnie posiada Zamawiający, Wykonawca w cenie oferty na dostawę licencji na oprogramowanie do ochrony antywirusowej zobowiązany jest uwzględnić wszystkie koszty wdrożenia oferowanego oprogramowania oraz zobowiązany jest do:

- instalacji centralnej konsoli zarządzania,
- zapewnienia przeszkolenia personelu informatycznego Zamawiającego w zakresie używania, zarządzania oraz administrowania programem antywirusowym i konsolą centralnego zarządzania,
- instalacji oprogramowania agenta na stacjach klienckich,
- instalacji / uruchomienia konsoli centralnego zarządzania dla oferowanego rozwiązania antywirusowego.

Czas realizacji: 14 dni od daty podpisania umowy.