OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Przedmiotem zamówienia jest: „Zakup przedłużenie licencji oprogramowania do ochrony antywirusowej dla potrzeb użytkowanych stanowisk roboczych w jednostkach Policji garnizonu mazowieckiego” – zgodnych z poniższymi wymaganiami Zamawiającego.

Licencja na aktualnie posiadane oprogramowanie **ESET Endpoint Antyvirus obowiązuje do dnia 17.03.2022 roku**. **Wykonawca zobowiązuje się do dostarczenia przedmiotu zamówienia w postaci klucza licencyjnego oraz linku do pobierania oprogramowania na wskazany adres e-mail w terminie najpóźniej do dnia 17.03.2022r**., oraz jego realizacji na warunkach określonych w niniejszym OPZ oraz wzorze Umowy z zachowaniem ciągłości ochrony antywirusowej. Dostarczone licencje mają obowiązywać przez okres kolejnych 12 miesięcy licząc od daty upływu ich ważności i posiadać 12 miesięczną gwarancję producenta.

Obecne oprogramowanie:

Zamawiający obecnie użytkuje licencje oprogramowania antywirusowego ESET Endpoint Antivirus na 3000 stanowisk roboczych. W związku z upływającym terminem posiadanej - wykupionej licencji na wyżej wymienionej liczbie stanowisk, Zamawiający zamierza przedłużyć posiadaną licencję ESET Endpoint Antivirus tylko na 220 stanowisk roboczych, tak aby mógł użytkować oprogramowanie przez okres kolejnych 12 miesięcy. Numer posiadanej licencji Zamawiający udostępni na żądanie Wykonawcy lub w momencie podpisania Umowy z Wykonawcą.

Oprogramowanie musi posiadać:

1. Wsparcie dla systemu Windows 8, Windows 10, wsparcie dla 32 i 64 - bitowej wersji systemu Windows.
2. Wersja programu dla stacji roboczych Windows dostępna w języku polskim.

Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wbudowana technologia do ochrony przed rootkitami.
3. Wykrywanie potencjalnie niepodanych, niebezpiecznych oraz podejrzanych aplikacji.
4. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
5. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak - nie wykonywało danego zadania.

6. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami
7. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).
8. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
9. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
10. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
11. Wbudowany konektor dla programów MS Outlook, Outlook Express, (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).
12. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
13. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
14. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
15. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
16. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
17. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
18. 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.
19. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
20. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji - poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.
21. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
22. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.

23. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
24. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
25. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
26. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
27. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
28. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
29. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http.
30. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
31. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.