Załącznik nr 2 do umowy

Opis przedmiotu zamówienia

Obecnie Centrum Projektów Europejskich posiada oprogramowanie antywirusowe ESET Endpoint Antyvirus Suite, który według producenta zmienił nazwę na ESET PROTECT Essential ON-PREM. Przedmiotem zamówienia jest **odnowienie licencji na 220 urządzeń na oprogramowanie antywirusowe ESET na okres 36 miesięcy**. Identyfikator aktualnej licencji EAV-0220434057. Optymalnym rozwiązaniem byłoby przedłużenie posiadanej licencji, jednak Zamawiający dopuszcza możliwość zaoferowania produktów równoważnych w zakresie nowej licencji na oprogramowanie antywirusowe (oprogramowanie równoważne). Przy zmianie oprogramowania musi być zapewnione wsparcie w zakresie migracji, instalacji (w siedzibie Zamawiającego w Warszawie, ul. Domaniewska 39a oraz w Krakowie, Gdańsku, Wrocławiu i Olsztynie) przez Wykonawcę lub Producenta oprogramowania na czas zaplanowanego wdrożenia przez Zamawiającego na wszystkich wymaganych urządzeniach (około 220 urządzeń). Koszt migracji, instalacji i wdrożenia nowego oprogramowania musi być wliczony w cenę licencji. Migracja i instalacja zmienionego oprogramowania musi zostać wykonana w terminie 7 dni od dnia dostawy oprogramowania.

Zamawiający dopuszcza produkt równoważny, którego funkcjonalność pokrywa się z funkcjami ESET PROTECT Essential ON-PREM. W przypadku rozwiązania równoważnego Zamawiający wymaga przeprowadzenia przez wykonawcę migracji, instalacji i wdrożenia oprogramowania (instalacja na wszystkich stanowiskach wskazanych przez Zamawiającego) oraz przeprowadzenie szkolenia informatyków (2 osoby) w zakresie obsługi oprogramowania.

Równoważność oznacza, że:

a. oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem (Windows 7, 8, 10, Windows Server 2008, 2008 R2, 2012, 2012 R2, 2019, 32-bit oraz 64-bit) i sprzętem funkcjonującym u Zamawiającego;

b. oprogramowanie równoważne musi zapewniać co najmniej pełną funkcjonalność oprogramowania w stosunku, do którego jest wskazywana przez wykonawcę jako równoważne i posiadać co najmniej takie same parametry techniczne i funkcjonalne;

c. warunki licencji oprogramowania równoważnego w każdym aspekcie licencjonowania muszą być nie gorsze niż licencje oprogramowania wskazanego przez Zamawiającego w stosunku do którego jest równoważna;

d. warunki i zakres licencji dla oprogramowania równoważnego muszą być nie gorsze niż dla oprogramowania wskazanego przez Zamawiającego w stosunku do którego jest równoważna.

3. Zamawiający wymaga, aby wykonawca w formularzu ofertowym opisał wszystkie dane techniczne składające się na dany asortyment zgodnym z zamówieniem.

Uwaga:
1) W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne".
2) W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania

równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.
4) Wykonawca, który powoła się na oprogramowanie równoważne w zakresie opisanym przez Zamawiającego, jest obowiązany wykazać w ofercie, że oferowany przez niego przedmiot dostawy spełnia wymagania określone przez Zamawiającego.
5) Ciężar dowodowy w zakresie udowodnienia równoważności zaoferowanego oprogramowania z opisanymi warunkami równoważności spoczywa na Wykonawcy, składającym ofertę równoważną.
6) Zamawiający wymaga, aby zaoferowane przez Wykonawcę oprogramowanie równoważne nie powodowało konieczności wykonania dodatkowych prac integracyjnych po stronie Zamawiającego, tym samym poniesienia dodatkowych, niezaplanowanych kosztów.
7) W celu potwierdzenia, iż oferowana dostawa spełnia wymagania określone przez Zamawiającego, Wykonawca, który zaoferuje oprogramowanie równoważne do wskazanego przez Zamawiającego załączy do oferty szczegółową specyfikację techniczną dla oferowanego oprogramowania równoważnego, wystawioną przez producenta oferowanego oprogramowania równoważnego, zawierającą opis wszystkich cech i funkcjonalności oferowanego oprogramowania równoważnego.
8) Oprogramowanie musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego oprogramowania nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.

Obecnie użytkowane przez Zamawiającego oprogramowanie antywirusowe zapewnia poniższe funkcje:

1. **Ochrona urządzeń mobilnych opartych o System Android co najmniej w wersji 7.0.**
    1) Ochrona antywirusowa plików w czasie rzeczywistym
    2) Ochrona przed atakami typu „phishing”
    3) Skanowanie plików archiwum oraz innych
    4) Skanowanie nośników zainstalowanych w urządzeniu kart pamięci SD
    5) Aplikacja ma mieć możliwość określenia poziomu głębokości skanowania plików archiwum
    6) Aplikacja ma mieć możliwość określenia domyślnej akcji podejmowanej w przypadku wykrycia zagrożenia: przeniesienia do kwarantanny, usunięcia lub zignorowania
    7) W przypadku wykrycia zagrożenia użytkownik ma otrzymać odpowiednie powiadomienie
    8) Aplikacja musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia
    9) Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji
    10) Ochrona przed kradzieżą
    11) Użytkownik ma mieć możliwość wprowadzenia zaufanej karty SIM
    12) Aplikacja ma mieć możliwość wprowadzenia zaufanych odbiorców wiadomości, do których zostanie przesłana informacja w przypadku umieszczenia w urządzeniu innej niż zaufana karty SIM
    13) W przypadku kradzieży urządzenia, administrator Systemu ma mieć możliwość wysłania na urządzenie komendy, która umożliwi usunięcie zawartości urządzenia, zablokowania urządzenia, przesłania na zaufany numer telefonu lokalizacji GPS w której skradzione urządzenie się znajduje.
    14) Administrator musi mieć możliwość wysyłania powyższych komend bezpośrednio z poziomu konsoli centralnego zarządzania.
    15) Możliwość zdalnego zresetowania hasła ma być możliwa tylko w przypadku wysłania odpowiedniego polecenia z zaufanego urządzenia.

16) Aplikacja musi posiadać funkcjonalność pozwalającą administratorowi na monitorowanie ustawień urządzenia w celu weryfikacji czy są one zgodne z polityką.
17) Kontrola aplikacji musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji
18) Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji

2. Ochrona stacji roboczych oraz Serwerów z pełnym wsparciem dla systemu Windows 7, 8, 10, Windows Server 2008, 2008 R2, 2012, 2012 R2, 2019, 32-bit oraz 64-bit

1) Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim
2) Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3) Wbudowana technologia do ochrony przed rootkitami.
4) Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5) Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6) Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7) 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.
8) Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9) Możliwość skanowania dysków sieciowych i dysków przenośnych.
10) Skanowanie plików spakowanych i skompresowanych.
11) Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
12) Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku ale również ma być możliwe użycie symbolu wieloznacznego „*” zastępującego dowolne znaki w ścieżce.
13) W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
14) Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
15) Wbudowany konektor dla programów MS Outlook.
16) Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook.
17) 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).
18) Automatyczna integracja skanera POP3 i IMAP z klientem pocztowym MS Outlook bez konieczności zmian w konfiguracji.
19) Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić

blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.

20) Automatyczna integracja z przeglądarką internetową Google Chrome oraz Microsoft Edge bez konieczności zmian w konfiguracji.
21) Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
22) Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
23) Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
24) Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, czytników kart inteligentnych, modemów, urządzeń przenośnych.
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) Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
28) Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
29) Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.
30) Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, 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.
32) Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.
33) Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
34) W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.
35) Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła administratora.

3. Administracja zdalna konsola

1) Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2019 oraz Linux

2) Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.
3) Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
4) Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.
5) Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
6) Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.
7) Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.
8) Komunikacja z konsolą powinna być zabezpieczona za pośrednictwem protokołu SSL.
9) Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
10) Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
11) Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
12) Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
13) Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
14) Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, oraz Linux oraz serwerach Windows.
15) Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
16) Centralna konfiguracja i zarządzanie ochroną antywirusową i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
17) Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
18) Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
19) Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej.
20) Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
21) Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego.
22) Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
23) W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
24) Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.

25) Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.
26) Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.
27) Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
28) Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
29) Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
30) Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
31) Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.
32) Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
33) Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
34) Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.
35) Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
36) Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
37) Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.
38) Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.
39) Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
40) Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.
41) Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.
42) Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi

oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.

43) Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
44) Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś" dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.
45) Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.
46) Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta.
47) Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
48) Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
49) Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp.
50) Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
51) Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
52) Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
53) Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
54) Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 lub wyszukania konkretnej nazwy zagrożenia.
55) Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań.
56) Konfiguracja zestawów uprawnień musi umożliwiać przypisanie praw tylko do odczytu, odczytu i użycia, oraz prawo do zapisania zmian w ramach danego zadania lub polityki w konsoli.