Opis Przedmiotu Zamówienia
Zakup wsparcia

1. Wymagania ogólne

1) Kontrakty serwisowe muszą zapewniać:

   a) Dostęp do aktualizacji oprogramowania i możliwość aktualizacji oraz możliwości zmiany jego wersji na nowszą, gdy taka zostanie wydana przez producenta oprogramowania;
   b) Naprawę wszystkich Wad poprzez aktualizację lub za zgoda Zamawiającego poprzez zastosowanie rozwiązania zastępczego.

2) Wykonawca zobowiązuje się do świadczenia w ramach Usługi Wsparcia Technicznego przez konsultantów Wykonawcy bieżących konsultacji telefonicznych w zakresie eksploatacji Urządzeń, w szczególności przez wyjaśnienia, diagnozy, porady i odpowiedzi na pytania związane z eksploatacją Urządzeń. Jak również pomocy w przypadku trudności z wykonaniem prac administracyjnych i konfiguracyjnych.
3) Wsparcie producenta dla Urządzeń musi być potwierdzone przez polskie lub regionalne przedstawicielstwo/oddział producenta Oprogramowania.
4) W ramach dostarczonych kontraktów serwisowych i świadczonej na rzecz Zamawiającego Usługi Wsparcia Technicznego Wykonawca będzie nieodpłatnie usuwał wszystkie wady oprogramowania.
5) Wykonawca zobowiązuje się realizować usługę z zachowaniem podanych terminów realizacji z najwyższą starannością, z uwzględnieniem profesjonalnego charakteru prowadzonej przez Wykonawcę działalności.
6) Wady Oprogramowania będą zgłaszane przez Zamawiającego za pomocą faksu lub telefonu lub poczty elektronicznej przekazanej na wskazane adresy lub numery telefonów kontaktowych Wykonawcy.
7) Wykonawca będzie przyjmował Zgłoszenia Serwisowe przez 5 dni w tygodniu (od poniedziałku do piątku z pominięciem weekendów i Świąt) w godzinach 7:30- 15:30.
8) Wykonawca - poza przypadkami, gdy samodzielnie wykryje Wadę o nienależytym wykonywaniu umowy lub niewykonaniu umowy, a także o wszelkich innych Wadach, zostanie poinformowany przez Zamawiającego drogą:

   a) telefoniczną – na numer telefonu Wykonawcy:....., lub
   b) telefoniczną – na numer faksu Wykonawcy:....., lub
   c) elektroniczną – na adres e-mail Wykonawcy:.....

9) Informacja o nienależytym wykonywaniu umowy lub niewykonaniu umowy, a także o wszelkich Wadach lub Kontraktów Serwisowych zostanie uznana za dostarczoną w przypadku przekazania jej

za pomocą jednego z kanałów komunikacyjnych, o których mowa w pkt 9. Przekazanie informacji jednym ze sposobów, o których mowa w pkt 9, nie wyklucza zastosowania innych sposobów wymienionych w tym ustępie lub innych sposobów w nim nie wskazanych (np. doręczenie za pomocą poczty czy doręczenie osobiste).

2. Oprogramowanie zgodne z posiadanym przez Zamawiającego

Przedmiotem zamówienia jest dostawa:

1) kontraktu na usługę wsparcia technicznego producenta dla posiadanego przez Zamawiającego oprogramowania ESET Endpoint Security 7.0 (zarejestrowanych na koncie Gminy Wrocław i jej jednostek) dla licencji opisanych w punkcie 2.

2) licencji Symantec ESET Endpoint Security 7.3:

Okres licencji oraz wsparcia tech.	Ilość
13.01.2021-12.01.2024	4560

3) voucherów (ważnych co najmniej do 31.12.2021) uprawniających dwóch pracowników wskazanych przez Zamawiającego do odbycia szkoleń w zakresie instalacji, konfiguracji, diagnostyki i zarządzania systemem antywirusowym.

3. Oprogramowanie równoważne

W przypadku wdrożenia przez Wykonawcą oprogramowania innego niż posiadane przez Zamawiającego należy dostarczyć zintegrowaną ochronę stacji końcowych, która musi charakteryzować się następującymi funkcjonalnościami:

- Inteligentny sposób zarządzania — scentralizowana administracja i zautomatyzowane procesy zarządzania,
- Ochrona przed zagrożeniami pochodzącymi z sieci tj. "zapora ogniowa" oparta na regułach,
- Ochrona przeglądarek WWW oraz funkcja blokowania luk w zabezpieczeniach,
- Filtrowanie adresów URL przed złośliwymi adresami,
- konsolidacja wielu zadań w agencie na stacji końcowej (funkcja ochrony antywirusowej, "zapora ogniowa", zapobiegania próbom ataków oraz kontroli dostępu do urządzeń, aplikacji i sieci),
- Ochrona w czasie rzeczywistym przed nieznanymi stronami WWW wyłudzającymi informacje,
- Statyczne i heurystyczne wykrywanie podejrzanych elementów w witrynach,
- Silniki detekcji oparte nie tylko o sygnatury, ale także heurystyke i zachowania,
- Wykrywanie i blokowanie komunikacji „Command&Control” z zainfekowanych komputerów,
- Automatyczna ochrona antywirusowa plików otwartych lub używanych na komputerze z możliwością konfiguracji procesów zaufanych (niewymagających ochrony),
- Wykrywanie i usuwanie potencjalnie niebezpiecznych aplikacji tzw. Riskware (keylogger, narzędzia zdalnej kontroli, itp.),
- Ochrona przed wirusami i programami typu „spyware”,
- Cykliczne skanowanie komputera zgodne z regułami dotyczącymi cyklu i czasu skanowania, możliwość przerwania skanowania przez użytkownika, obszarów krytycznych systemu, nośników

wymiennych, dysków optycznych, archiwów plików, plików niewykonywanych oraz rozmiaru plików,
- Skanowanie komputera z uwzględnieniem optymalizacji,
- Skanowanie komputera z obniżeniem priorytetu względem zadań wykonywanych przez użytkownika,
- Polityka ochrony przed oprogramowanie złośliwym skoordynowana z Active Directory
- Możliwość definiowania wykluczeń na podstawie ścieżki położenia pliku,
- Definiowanie elementów, które użytkownik może widzieć i zmienić na poziomie agenta np. wyłączenie modułu bezpieczeństwa lub powiadomień,
- Rezultat skanowanie powinien zawierać co najmniej: nazwa zagrożenia, typ zagrożenia, wynik akcji,
- Kontrola (wraz z raportowaniem), w tym blokada podłączonych urządzeń do komputera tj. nośników zewnętrznych takich jak: pendrive'y telefony, aparaty fotograficzne, zewnętrzne dyski,
- Zapora ogniowa umożliwiająca definiowanie reguł dla ruchu przychodzącego i wychodzącego,
- Zapora ogniowa powinna posiadać możliwość definiowania następujących parametrów polityce bezpieczeństwa jak: adres źródłowy, adres docelowy, protokół, usługa,
- Zezwalane zaufanym aplikacjom na dostęp do Internetu, blokowanie dostępu specyficznym aplikacjom do Internetu lub brak możliwości uruchomienia aplikacji na komputerze
- Możliwość kontroli aplikacji na podstawie bazy reputacji dostarczanej przez producenta
- Weryfikacja spełnienia zgodności komputera z obowiązującymi zasadami w organizacji w zakresie:
    - Weryfikacji, czy moduły zintegrowanej ochrony są uruchomione
    - Weryfikacji wpisów w rejestrze systemowym
    - Weryfikacji istnienia plików poprzez weryfikację ścieżki sumy kontrolnej
    - Wykonywanie operacji w przypadku wykrycia niezgodności poprzez ostrzeżenie zarejestrowane w logu
    - Wykrywanie aplikacji zabronionych i podejmowania działań umożliwiających zablokowanie, zarejestrowanie w logu lub usunięcie

W ramach wdrożenia do obowiązków Wykonawcy należy:

• Wykonanie instalacji i konfiguracji serwera zarządzającego na maszynie wirtualnej Vmware ESX,
• Przygotowanie paczek instalacyjnych oprogramowania klienckiego wraz z zintegrowanym agentem
• Konfiguracja polityk,
• Stworzenie grup statycznych,
• Pomoc przy usunięciu obecnego antywirusa,
• Instalacja wcześniej przygotowanej paczki klienta wraz z agentem na komputerach Zamawiającego,
• Weryfikacja przypisana odpowiednich polityki/ konfiguracja,
• Weryfikacja poprawności instalacji,
• Przygotowanie dokumentacji powdrożeniowej,
• Przeprowadzenie szkolenia dla administratorów.

4. Harmonogram rzeczowy

Typ zamówienia	Początek obowiązywania licencji	Koniec obowiązywania licencji	Ilość licencji
podstawowe	13.01.2021	12.01.2024	4560
Dodatkowe (opcje)	od dnia dostarczenia	na okres 3 lat	1000