

Załącznik 1 do zapytania ofertowego dla zadania:

Dostawa oprogramowania antywirusowego dla Miejskiego Zarządu Budynków Mieszkalnych w Dąbrowie Górniczej.

Szczegółowy opis przedmiotu zamówienia (OPZ)

Przedmiotem zamówienia jest zakup i dostawa systemu ochrony antywirusowej dla 80 stacji roboczych wraz z centralnym systemem zarządzania dla systemów Windows 10/11/Serwer-22, aktualizacjami baz sygnatur, wsparciem technicznym producenta .

1. Zamówienie obejmuje:

- a. Dostawę licencji dla 80 stanowisk komputerowych.
- b. Instalacja i konfiguracja konsoli administracyjnej.
- c. Szkolenie administratorów.

2. Wymagania ogólne

- a. Licencje muszą pochodzić z oficjalnego kanału dystrybucji producenta.
- b. Oprogramowanie musi być objęte pełnym wsparciem producenta.
- c. Rozwiązanie musi umożliwiać rozbudowę o dodatkowe stanowiska bez konieczności wymiany konsoli zarządzającej.
- d. Producent musi zapewniać regularne aktualizacje baz sygnatur i silników detekcji.

3. Wymagania funkcjonalne

a. Ochrona stacji roboczych - Rozwiązanie musi zapewniać:

- ochronę antywirusową w czasie rzeczywistym,
- ochronę przed ransomware,
- ochronę przed spyware,
- ochronę przed rootkitami,
- ochronę przed exploitami,
- ochronę przed phishingiem,
- ochronę przed atakami wykorzystującymi skrypty PowerShell,
- ochronę przed zagrożeniami typu fileless malware,
- ochronę przed nieautoryzowanym szpiegowaniem danych.

b. Technologie detekcji - Wymagane jest wykorzystanie:

- sygnatur zagrożeń,
- analizy heurystycznej,
- analizy behawioralnej,
- uczenia maszynowego,
- systemu reputacyjnego opartego na chmurze producenta,
- mechanizmów wykrywania zagrożeń typu zero-day.

c. Ochrona sieciowa - Rozwiązanie musi posiadać:

- zaporę osobistą (Personal Firewall),
- ochronę przed atakami sieciowymi,
- wykrywanie prób włamań,
- ochronę przed skanowaniem portów,

-możliwość definiowania reguł komunikacji.

d. Ochrona użytkownika - Rozwiązanie musi zapewniać:

- ochronę poczty elektronicznej,
- ochronę przeglądarek internetowych,
- ochronę przed stronami phishingowymi,
- ochronę bankowości internetowej,
- ochronę transakcji elektronicznych.

e. Kontrola urządzeń- System musi umożliwiać:

- kontrolę pamięci USB,
- blokowanie urządzeń zewnętrznych,
- definiowanie wyjątków dla określonych urządzeń,
- prowadzenie rejestru podłączanych urządzeń.

4. Centralna konsola zarządzania - Zamawiający wymaga centralnego systemu zarządzania dostępnego przez przeglądarkę internetową, która musi umożliwiać:

- zarządzanie wszystkimi stacjami roboczymi,
- tworzenie grup komputerów,
- tworzenie polityk bezpieczeństwa,
- zdalną instalację oprogramowania,
- zdalną aktualizację klientów,
- zdalne uruchamianie skanowania,
- podgląd incydentów bezpieczeństwa,
- generowanie raportów,
- eksport raportów do PDF i CSV,
- wysyłanie alertów pocztą elektroniczną,
- zarządzanie rolami administratorów.

5. Integracja z infrastrukturą Zamawiającego - Rozwiązanie musi umożliwiać:

- integrację z Microsoft Active Directory,
- automatyczną synchronizację użytkowników i grup,
- uwierzytelnianie administratorów z wykorzystaniem Active Directory,
- wdrożenie agentów z poziomu konsoli.

6. Wymagania dotyczące raportowania - System musi umożliwiać generowanie raportów obejmujących:

- wykryte zagrożenia,
- stan aktualizacji,
- aktywność użytkowników,
- podłączone urządzenia USB,
- komputery nieposiadające aktualnych baz sygnatur,
- historię incydentów bezpieczeństwa.

7. Licencjonowanie

- a. Licencja dla 80 stanowisk komputerowych.
- b. Licencja ważna przez 12 miesięcy.
- c. Aktualizacje silników detekcji przez cały okres obowiązywania licencji.
- d. Brak ograniczeń funkcjonalnych w okresie licencyjnym.
- e. Możliwość rozbudowy o dodatkowe stanowiska.

8. Dostawa oprogramowania

- a. Wykonawca zobowiązany jest do dostarczenia oprogramowania w postaci elektronicznej(cyfrowej), bez dostawy nośników fizycznych.
- b. Dostawa obejmuje w szczególności:
 - klucze/licencje aktywacyjne,
 - dane umożliwiające dostęp do portalu producenta lub konsoli zarządzającej (jeżeli są wymagane),
 - dokument potwierdzający udzielenie licencji na okres 12 miesięcy,
 - instrukcję aktywacji lub uruchomienia oprogramowania (jeżeli jest wymagana).

Wymienione materiały należy przesłać drogą elektroniczną na adres e-mail Zamawiającego:

informatycy@mzbm.com.pl.

Za termin dostarczenia przedmiotu zamówienia uznaje się dzień skutecznego doręczenia wiadomości e-mail zawierającej komplet wymaganych danych i dokumentów umożliwiających korzystanie z oprogramowania zgodnie z warunkami zamówienia.

9. Termin realizacji

Wykonawca zobowiązany jest do realizacji zamówienia w terminie nie dłuższym niż 14 dni od daty podpisania umowy.

10. Wymagania wobec wykonawcy

Wykonawca zobowiązany jest:

- posiadać status partnera producenta oferowanego rozwiązania lub równoważny,
- posiadać doświadczenie w realizacji minimum trzech wdrożeń systemów ochrony w okresie ostatnich trzech lat.

11. Gwarancja i wsparcie producenta

1. Wykonawca udzieli gwarancji na dostarczone licencje oprogramowania na cały okres obowiązywania licencji, nie krótszy niż 12 miesięcy od dnia podpisania protokołu odbioru.
2. W okresie obowiązywania gwarancji i licencji Zamawiający musi mieć zapewnione:
 - dostęp do wszystkich aktualizacji baz sygnatur zagrożeń oraz silnika skanującego,
 - dostęp do nowych wersji oprogramowania udostępnianych przez producenta bez dodatkowych opłat,
 - wsparcie techniczne producenta lub autoryzowanego partnera producenta w języku polskim, realizowane drogą elektroniczną oraz telefoniczną,
 - możliwość zgłaszania problemów technicznych oraz uzyskiwania pomocy w zakresie instalacji, konfiguracji i eksploatacji oprogramowania.
3. Dostarczone licencje muszą pochodzić z oficjalnego kanału dystrybucji producenta, być fabrycznie nowe, nieużywane oraz umożliwiać korzystanie z pełnej funkcjonalności

oprogramowania zgodnie z warunkami licencyjnymi producenta. W okresie ważności licencji użytkownik zachowuje prawo do aktualizacji oraz korzystania ze wsparcia technicznego.