ZAŁĄCZNIK NR 2
do ZP/2311/06/239/2023

OPIS PRZEDMIOTU ZAMÓWENIA

Wymaganie minimalne dotyczące oprogramowania będącego przedmiotem Zapytania ofertowego Nr ZP/2311/06/239/2023

1. **Wspierane systemy operacyjne:**

System Operacyjny Windows:

- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1

Systemy operacyjne serwerowe

- Windows Server 2022
- Windows Server 2019 Core
- Windows Server 2019
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

Systemy Operacyjne Linux

- CentOS 7.x
- CentOS 8.x
- Debian 9
- Debian 10
- Debian 11
- Ubuntu 16.04.x
- Ubuntu 18.04.x
- Ubuntu 20.04.x

- Ubuntu 21.04.x
- Ubuntu 21.10.x
- Ubuntu 22.04.x

2. Szczegółowe cechy oprogramowania :

1) Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami
2) Czas obowiązywania licencji na oprogramowanie - 36 miesięcy
3) Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim
4) Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi
5) Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
6) Wbudowana technologia do ochrony przed rootkitami.
7) Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8) Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
9) Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10) Możliwość skanowania dysków sieciowych i dysków przenośnych.
11) Skanowanie plików spakowanych i skompresowanych.
12) Możliwość dodawania wykluczeń na podstawie:

    Plik

    b) Folder

    c) Rozszerzenie

    d) Proces

    e) Hash pliku

    f) Hash certyfikatu

    g) Nazwa zagrożenia

    h) Wiersz poleceń

    i) IP/maska

12) Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook
13) Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
14) Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.

15) Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
16) Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
17) Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.
18) Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
19) Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.
20) Praca programu musi być niezauważalna dla użytkownika.
21) Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.
22) Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie).
23) Wbudowany IDS.
24) Możliwość tworzenia list sieci zaufanych.
25) Możliwość dezaktywacji funkcji zapory sieciowej.
26) Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.
27) Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak:

    -Wczesny dostęp

    -Dostęp do poświadczeń

    -Wykrycie

    -Crimeware

28) Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej.
29) Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji.

3. Stacje robocze i serwery

1) Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2) Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3) Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
4) Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
5) Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
6) Skanowanie plików spakowanych i skompresowanych.
7) Oprogramowanie posiada możliwość zablokowania hasłem odinstalowania programu.
8) Produkt i sygnatury są aktualizowane nie rzadziej niż raz na godzinę.
9) Oprogramowanie posiada możliwość raportowania zdarzeń informacyjnych.
10) Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
11) Program musi posiadać możliwość skanowania jedynie nowych nie zmienionych plików.
12) Program musi mieć wbudowany skaner wyszukiwania rootkitów.
13) Możliwość odblokowania ustawień programu.
14) Możliwość zabezpieczenia klienta przed odinstalowaniem

4. Konsola zdalnej administracji - Konsola Cloud – serwer administracyjny po stronie producenta

1) Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.
2) Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego.
3) Możliwość integracji Domeny Active Directory
4) Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
5) Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
6) Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi
7) Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.
8) Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internet
9) W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.