**Zakup oprogramowania antywirusowego i konsoli administracyjnej – opis przedmiotu zamówienia**

**Wymagania ogólne:**

1. Oprogramowanie antywirusowe i konsola administracyjna jest w języku polskim.

2. Ilość Licencji: 200 szt. dla stacji roboczych oraz systemów serwerowych.

3. Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w

formie papierowej lub elektronicznej.

4. Zamawiający może korzystać z licencji edukacyjnych (typu Edu)

5. Oprogramowanie antywirusowe wspiera następujące systemu operacyjne:

* Microsoft Windows 10
* Microsoft Windows 11
* Microsoft Windows Server 2012 Standard
* Microsoft Windows Server 2012 Essentials
* Microsoft Windows Server 2012 Datacenter
* Microsoft Windows Server 2012 Core
* Microsoft Windows Server 2016 Standard
* Microsoft Windows Server 2016 Essentials
* Microsoft Windows Server 2016 Datacenter
* Microsoft Windows Server 2016 Core
* Microsoft Windows Server 2019 Standard
* Microsoft Windows Server 2019 Essentials
* Microsoft Windows Server 2019 Datacenter
* Microsoft Windows Server 2019 Core
* Microsoft Windows Server 2022 Standard
* Microsoft Windows Server 2022 Essentials
* Microsoft Windows Server 2022 Datacenter
* Microsoft Windows Server 2022 Core

6. Konsola administracyjna wspiera następujące systemy operacyjne:

* Microsoft Windows 10
* Microsoft Windows 11
* Microsoft Windows Server 2012 Standard
* Microsoft Windows Server 2012 Essentials
* Microsoft Windows Server 2012 Datacenter
* Microsoft Windows Server 2012 Core
* Microsoft Windows Server 2016 Standard
* Microsoft Windows Server 2016 Essentials
* Microsoft Windows Server 2016 Datacenter
* Microsoft Windows Server 2016 Core
* Microsoft Windows Server 2019 Standard
* Microsoft Windows Server 2019 Essentials
* Microsoft Windows Server 2019 Datacenter
* Microsoft Windows Server 2019 Core
* Microsoft Windows Server 2022 Standard
* Microsoft Windows Server 2022 Essentials
* Microsoft Windows Server 2022 Datacenter
* Microsoft Windows Server 2022 Core

7. Pełne wsparcie dla 64-bitowych systemów operacyjnych w przypadku oprogramowania antywirusowego jak i konsoli administracyjnej.

8. Wspierane przeglądarki internetowe do obsługi konsoli administracyjnej:

* Microsoft Edge
* Mozilla Firefox
* Google Chrome
* Opera

**Funkcjonalność programu:**

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, phishing, narzędzi hakerskich, backdoor, ransomware itp.

3. Wbudowana technologia do ochrony przed rootkitami.

4. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

5. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

6. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, pozalogowaniu i po uruchomieniu komputera).

7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.

8. Możliwość skanowania dysków sieciowych i dysków przenośnych.

9. Skanowanie plików spakowanych i skompresowanych.

10. 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.

11. Współpraca z programem antywirusowym Mozilla Thunderbird

12. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu Mozilla Thunderbird.

13. 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).

14. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.

15. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.

16. 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.

17. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.

18. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS,POP3S, IMAPS.

19. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.

20. 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.

21. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik korzystający zkomputera przy próbie dostępu do konfiguracji był proszony o podanie hasła.

22. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiadaona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać ohasło.

23. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji musibyć takie samo.

24. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).

25. 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.

26. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.

27. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacjibaz wirusów i samego oprogramowania.

28. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

**Konsola administracyjna – zakres funkcjonalny:**

1. Centralna instalacja programów służących do ochrony stacji roboczych Windows.

2. Centralne zarządzanie programami służącymi do ochrony stacji roboczych Windows

3. Centralna instalacja oprogramowania na końcówkach (stacjach roboczych) z systemami operacyjnymi wymienionymi w Wymaganiach ogólnych, w punkcie 5 z pełnym wsparciem dla systemów 64-bitowych.

4. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, zaporą osobistą i kontrolą dostępu do stron internetowych.

5. Możliwość uruchomienia centralnego skanowania wybranych stacji roboczych z opcją wygenerowaniaraportu ze skanowania i przesłania do konsoli zarządzającej.

6. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych).

7. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacjiroboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacjarobocza należy.

8. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.

9. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.

10. Możliwość importowania konfiguracji programu z wybranej stacji roboczej, a następnie przesłanie (skopiowanie) jej na inną stację lub grupę stacji roboczych w sieci.

11. Możliwość zmiany konfiguracji na stacjach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko, jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).

12. Możliwość uruchomienia serwera centralnej administracji i konsoli zarządzającej na systemach operacyjnych wymienionych w Wymaganiach ogólnych, w punkcie 6 z zachowaniem pełnego wsparcia dla systemów 64-bitowych.

13. Możliwość rozdzielenia serwera centralnej administracji od konsoli zarządzającej, w taki sposób, że serwer centralnej administracji jest instalowany na jednym serwerze/ stacji a konsola zarządzająca na tym samym serwerze i na stacjach roboczych należących do administratorów.

14. Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) w formacie HTML lub CSV.

15. Aplikacja musi posiadać funkcjonalność, która umożliwi przesłanie wygenerowanych raportów na wskazany adres email.

16. Serwer centralnej administracji ma oferować funkcjonalność synchronizacji grup komputerów z drzewem Active Directory. Po synchronizacji automatycznie są umieszczane komputery należące do zadanych grup w AD do odpowiadających im grup w programie. Funkcjonalność ta nie może wymagać instalacji serwera centralnej administracji na komputerze pełniącym funkcję kontrolera domeny.

17. Serwer centralnej administracji ma być wyposażony w mechanizm informowania administratora o wykryciu nieprawidłowości w funkcjonowaniu oprogramowania zainstalowanego na klientach w tym przynajmniej informowaniu o: wygaśnięciu licencji na oprogramowanie, o tym że zdefiniowany procent z pośród wszystkich stacji podłączonych do serwera ma nieaktywną ochronę, oraz że niektórzy z klientów podłączonych do serwera oczekują na ponowne uruchomienie po aktualizacji do nowej wersji oprogramowania.

18. Serwer centralnej administracji ma być wyposażony w wygodny mechanizm zarządzania licencjami,który umożliwi sumowanie liczby licencji nabytych przez użytkownika. Dodatkowo serwer mainformować o tym, ilu stanowiskową licencję posiada użytkownik i stale nadzorować ile licencji spośródpuli nie zostało jeszcze wykorzystanych.

19. Możliwość tworzenia repozytorium aktualizacji na serwerze centralnego zarządzania i udostępniania goprzez wbudowany serwer http.

20. Możliwość definiowania administratorów o określonych prawach do zarządzania serwerem administracji centralnej (w tym możliwość utworzenia administratora z pełnymi uprawnieniami lub uprawnienia tylko do odczytu).

21. W przypadku tworzenia administratora z niestandardowymi uprawnieniami możliwość wyboru modułów, do których ma mieć uprawnienia: zarządzanie grupami, powiadomieniami, politykami, licencjami oraz usuwanie i modyfikacja klientów, zdalna instalacja, generowanie raportów, usuwanie logów, zmiana konfiguracji klientów, aktualizacja zdalna, zdalne skanowanie klientów, zarządzanie kwarantanna na klientach.

22. Wszystkie działania administratorów zalogowanych do serwera administracji centralnej mają być logowane.

23. Administrator musi posiadać możliwość centralnego, tymczasowego wyłączenia wybranego modułu ochrony na stacji roboczej.

24. Centralne tymczasowe wyłączenie danego modułu nie może skutkować koniecznością restartu stacjiroboczej.

25. Aplikacja musi posiadać możliwość natychmiastowego uruchomienia zadania znajdującego się w harmonogramie bez konieczności oczekiwania do jego zaplanowanego czasu.