Załącznik nr 1

do zaproszenia do składania ofert

ZOOiI.042.6.2022.KK

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest **zakup licencji na oprogramowanie antywirusowe na okres 12 miesięcy.**

Parametry oprogramowania zostały określone w poniższym zestawieniu:

Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Ilość licencji	110 sztuk
Oprogramowanie antywirusowe	Wszystkie usługi bezpieczeństwa (oraz bazy danych) dostępne są w postaci jednego urządzenia wirtualnego, które obejmuje punkty końcowe całego środowiska.
Wsparcie systemów	System Operacyjny Windows: Systemy Operacyjne Komputerów Pełne wsparcie: Windows 11 Windows 10 Windows 8.1 Windows 8 Windows 7 Systemy operacyjne serwera Pełne wsparcie Windows Server 2019 Core Windows Server 2019 Windows Server 2016 Windows Server 2016 Core Windows Server 2012 R2 Systemy Operacyjne Linux Ubuntu 14.04 LTS lub wyższy Red Hat Enterprise Linux / CentOS 6.0 lub wyżej SUSE Linux Enterprise Server 11 SP4 lub wyższy OpenSUSE Debian 8.0 l lub wyższy Systemy Operacyjne Mac OS X macOS Big Sur(11.0) macOS Catalina (10.15) macOS Mojave (10.14) macOS High Sierra (10.13)

	macOS Sierra (10.12) OS X El Capitan (10.11) Wymagania Ochrony Mobile ● Apple iPhone i tablety iPad (iOS 8.1+) ● Smartfony i tablety z Google Android (4.2+)
Ochrona antywirusowa i antyspyware	1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami 2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim. 3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi 4. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog3 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 wykluczeni na podstawie a. Plik b. Folder c. Rozszerzenie d. Proces e. Hash pliku f. Hash certyfikatu g. Nazwa zagrożenia h. Wiersz poleceń i. IP/maska 13. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express. 14. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 15. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 16. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne

	powiadomienie. 17. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta. 18. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 19. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać. 20. Program umożliwia skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS. 21. Program skanuje ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 22. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program będzie pytał o hasło. 23. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : O programie" możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony. 24. W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników. 25. W GUI programu możliwość wyświetlenia kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia. 26. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. 27. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 28. Praca programu musi być niezauważalna dla użytkownika. 29. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej. 30. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet. 31. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej. 32. Możliwość odblokowania ustawień programu po wpisaniu hasła 33. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu 34. 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) 35. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu. 36. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp. 37. Funkcja Ochrony danych konfigurowana zdalnie przez administratora. 38. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows. 39. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.

	40. Wbudowany IDS. 41. Możliwość zainstalowania silnika pełnego, lekkiego ze sprawdzaniem reputacji plików w chmurze, lub wykorzystanie dodatkowej maszyny wirtualnej która przejmie rolę silnika skanującego. 42. Maszyna która przejmuję rolę silnika skanującego musi działać w trybach redundancji lub równej dystrybucji. 43. Aktualizacja maszyny skanującej musi obejmować oddzielną aktualizację nowych funkcji, ulepszeń, poprawek oraz oddzielną aktualizację systemu operacyjnego urządzenia wirtualnego. 44. Możliwość tworzenia list sieci zaufanych. 45. Możliwość dezaktywacji funkcji zapory sieciowej. 46. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu. 47. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware. 48. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji. 49. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań(konfigurowalne w politykach bezpieczeństwa). 50. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups. 51. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego. 52. 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. Formaty plików jakie mogą być odzyskane: 3fr|ai|arw|bay|cab|cdr|cer|cr2|crt|crw|dcr|der|dgn|dll| dng|doc|docm|docx|dwg|dxf|dxg|eps|erf|exe|indd| ini|jpe|jpeg|jpg|mdf|mef|mrw|msg|msi|nef|nrw|odb| odc|odm|odp|ods|odt|orf|p12|p7b|p7c|pdd|pdf|pef| pem|pfx|png|ppt|pptm|pptx|psd|pst|ptx|py|r3d|raf|rtf| rw2|rwl|sr2|srf|srw|tsf|wb2|wpd|wps|x3f|xlk|xls|xlsb| xlsm|xlsx|xml| Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania.
Zintegrowane zarządzanie aktualizacjami oprogramowania firm trzecich.	Wspierane systemy operacyjne Windows: • Windows 11 • Windows 10 • Windows 8.1 • Windows 8 • Windows Server 2022 • Windows Server 2019 • Windows Server 2016

	• Windows Server 2012 R2 Wspierane systemy operacyjne Linux (64-bit): • CentOS 7 • Red Hat Enterprise Linux REL 8 • SUSE Linux Enterprise 1) Możliwość działania w trybie automatycznym. a) Możliwość oszacowania brakujących łatek. b) Możliwość zaplanowania oddzielnej automatycznej instalacji w oparciu o kategorię poprawek (bezpieczeństwo / niezwiązane z zabezpieczeniami). c) Możliwość opóźnienia ponownego uruchomienia, jeśli instalacja łatki tego wymaga. 2) Rozwiązanie musi zezwalać na tryb manualny – wykrywanie i instalacje łatek na żądanie. 3) Rozwiązanie musi oferować możliwość podejrzenia wszystkich brakujących łatek ze środowiska. Informacje te zostaną zebrane w module zarządzania aktualizacjami. a) Rozwiązanie dostarcza możliwość sprawdzenia które punkty końcowe posiadają zainstalowane lub niezainstalowane aktualizacje. b) Rozwiązanie przesyła informacje zwrotne w przypadku niepowodzenia instalacji łatki. c) Rozwiązanie daje użytkownikowi możliwość szybkiej instalacji brakujących łatek na urządzeniu. d) Użytkownik powinien mieć możliwość dodania do czarnej listy jednej lub wielu łatek. 4) Rozwiązanie raportuje brakujące łatki z perspektywy punktu końcowego (zainstalowane/ brakujące na każdym punkcie końcowym). 5) Rozwiązanie będzie okresowo wysyłać powiadomienia jeśli punkty końcowe nie posiadają zainstalowanych łatek. 6) Rozwiązanie zapewni możliwość buforowania, w ten sposób łatki będą pobierane z Internetu tylko przez niektóre przypisane punkty końcowe. 7) System wyświetla pozostały czas do automatycznego ponownego uruchomienia w powiadomieniu zarządzania poprawkami. 8) Funkcja wykrywania i informowania o każdej nowej zainstalowanej aplikacji na punkcie końcowym i dostępnych dla niej aktualizacji. 9) Możliwość automatycznego usuwania aktualizacji które nie mają już zastosowania ponieważ punkt końcowy nie istnieje lub aplikacja została usunięta. 10) Możliwość usunięcia z listy łatek które nie są już dostępne chociaż są obecne na niektórych punktach końcowych. 11) Możliwość wyszukiwania i pobierania aktualizacji dla wspieranych dystrybucji Linux i powiązanych z nimi produktów.