Załącznik Nr 2.2. do zapytania znak ORG.271.1.2023

Załącznik do oferty

SZCZEGÓŁOWA INFORMACJA O OFEROWANYM PRZEDMIOCIE ZAMÓWIENIA

oprogramowanie antywirusowe i firewall na 27 stanowisk – licencja na okres 5 lat

Nazwa	Nazwa producenta i oznaczenie typu proponowanych urządzeń
Oprogramowanie antywirusowe i firewall	1. Producent ..... 2. Oznaczenie , które pozwoli na jednoznaczną identyfikacje produktu (np. symbol, kod produktu itd.).....

UWAGA: W poniższej tabeli należy potwierdzić, że oferowane oprogramowanie spełnia wymagania poprzez skreślenie niewłaściwej odpowiedzi.

		Wymagania	Potwierdzenie spełnienia wymogów
1	**Administracja zdalna**	1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.	Spełnia / Nie spełnia
		2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.	Spełnia / Nie spełnia
		3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.	Spełnia / Nie spełnia
		4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.	Spełnia / Nie spełnia
		5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.	Spełnia / Nie spełnia
		6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.	Spełnia / Nie spełnia
		7. Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android.	Spełnia / Nie spełnia
		8. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.	Spełnia / Nie spełnia
		9. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).	Spełnia / Nie spełnia
		10. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania	Spełnia / Nie spełnia

		zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.	
		11. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.	Spełnia / Nie spełnia
		12. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.	Spełnia / Nie spełnia
		13. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.	Spełnia / Nie spełnia
		14. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.	Spełnia / Nie spełnia
		15. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.	Spełnia / Nie spełnia
		16. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.	Spełnia / Nie spełnia
2	**Ochrona stacji roboczych**	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11).	Spełnia / Nie spełnia
		2. Rozwiązanie musi wspierać architekturę ARM64.	Spełnia / Nie spełnia
		3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.	Spełnia / Nie spełnia
		4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.	Spełnia / Nie spełnia
		5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.	Spełnia / Nie spełnia
		6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	Spełnia / Nie spełnia
		7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.	Spełnia / Nie spełnia
		8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.	Spełnia / Nie spełnia
		9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.	Spełnia / Nie spełnia
		10. Rozwiązanie musi zapewniać 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).	Spełnia / Nie spełnia

11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.	Spełnia / Nie spełnia
12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.	Spełnia / Nie spełnia
13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.	Spełnia / Nie spełnia
14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.	Spełnia / Nie spełnia
15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: (poniżej jest wymienionych 9 pozycji)	Spełnia / Nie spełnia
• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,	Spełnia / Nie spełnia
• tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,	Spełnia / Nie spełnia
• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,	Spełnia / Nie spełnia
• tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,	Spełnia / Nie spełnia
• tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.	Spełnia / Nie spełnia
• tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,	Spełnia / Nie spełnia
• tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,	Spełnia / Nie spełnia
• tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,	Spełnia / Nie spełnia
• tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.	Spełnia / Nie spełnia
16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.	Spełnia / Nie spełnia
17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są	Spełnia / Nie spełnia

		podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.	
		18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.	Spełnia / Nie spełnia
		19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).	Spełnia / Nie spełnia
		20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.	Spełnia / Nie spełnia
		21. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego MS Outlook.	Spełnia / Nie spełnia
		22. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:	Spełnia / Nie spełnia
		23. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.	Spełnia / Nie spełnia
		24. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.	Spełnia / Nie spełnia
		25. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.	Spełnia / Nie spełnia
		26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.	Spełnia / Nie spełnia
		27. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.	Spełnia / Nie spełnia
		28. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.	Spełnia / Nie spełnia
		29. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.	Spełnia / Nie spełnia
3	**Ochrona serwera**	1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux.	Spełnia / Nie spełnia
		2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.	Spełnia / Nie spełnia
		3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.	Spełnia / Nie spełnia
		4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.	Spełnia / Nie spełnia
		5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.	Spełnia / Nie spełnia
		6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.	Spełnia / Nie spełnia

		7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.	Spełnia / Nie spełnia
		8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.	Spełnia / Nie spełnia
4	Dodatkowe wymagania dla ochrony serwerów Windows:	9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.	Spełnia / Nie spełnia
		10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).	Spełnia / Nie spełnia
		11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.	Spełnia / Nie spełnia
		12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.	Spełnia / Nie spełnia
		13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek	Spełnia / Nie spełnia

.....

(podpis Wykonawcy)

WÓJT
Wiesław Kulasza