ZAŁĄCZNIK NR 1

Oprogramowanie antywirusowe

Lp.	Nazwa komponentu	Parametry wymagane
1	Oprogramowanie antywirusowe	Oprogramowanie antywirusowe dla stacji roboczych oraz 4 serwerów – 50 licencji na okres do dnia 30 czerwca 2026 r.
2	Parametry minimalne	1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu przeglądarki internetowej za pomocą protokołu HTTPS. 3. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi. 4. Rozwiązanie musi posiadać możliwość tworzenia grup komputerów. 5. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11) oraz wspierać architekturę ARM64. 6. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 7. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 8. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 9. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 10. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 11. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 12. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików i katalogów. 13. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP w czasie rzeczywistym 14. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 15. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji: 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. 16. Rozwiązanie musi czerwca posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać administratorowi

		tworzenie reguł dla podłączanych urządzeń w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 18. Funkcja, generująca logi, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 19. Rozwiązanie musi posiadać chmurową wersję rozwiązania sandbox do którego będą przesyłane pliki lub części kodu przez użytkownika lub w sposób automatyczny 20. Rozwiązanie sandbox musi uruchomiać wskazane pliki przez użytkownika lub pliki, części kodu wysłane z serwerów Zamawiającego i stacji roboczych Zamawiającego i testować je pod względem bezpieczeństwa. Wynik testów musi być widoczny w konsoli administracyjnej Rozwiązania. Rozwiązanie musi jednocześnie po uzyskaniu wyniku zablokować dostęp do danego pliku jeżeli wynik wskaże na zagrożenie znajdujące się w danym pliku lub dać dostęp do wykonywania pliku jeżeli testy wykażą że plik jest bezpieczny. 21. Rozwiązanie musi posiadać automatyczną aktualizację silnika detekcji. 22. Rozwiązanie musi posiadać funkcjonalność skanera UEFI. 23. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. 24. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 25. Rozwiązanie musi posiadać możliwość filtrowania adresów URL. 26. Rozwiązanie musi zapewniać ochronę przed zagrożeniami zero-day. 27. 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. 28. 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 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, 29. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 30. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 31. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.

		32. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 33. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. 34. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 35. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście. 36. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 37. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 38. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup. 39. Rozwiązanie musi oferować system szyfrowania danych, który musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit. 40. Aplikacja musi posiadać autentykacje typu Pre-boot. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 41. Rozwiązanie musi posiadać moduł XDR dla systemów Windows, MacOS oraz linux, współpracujący z systemem do ochrony stacji roboczych/serwerów. 42. Rozwiązanie musi współpracować z serwerem administracyjnym produktu antywirusowego znajdującym się w chmurze. 43. Rozwiązanie musi posiadać serwer administracyjny działający w chmurze z możliwością wysyłania zdarzeń do konsoli administracyjnej. 44. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 45. Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia. 46. Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 47. Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne, pobrania do analizy oraz ich zablokowania. 48. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 49. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.

		50. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności.