



Opis przedmiotu zamówienia

Przedłużenie ważności licencji na oprogramowanie antywirusowe dla stacji roboczych i serwerów

I. Informacje ogólne

1. Przedmiotem zamówienia jest:
 - a. Przedłużenie ważności licencji o 1 rok na posiadane przez Zamawiającego oprogramowanie antywirusowe,
 - b. Zwiększenie ilości licencji na ww. oprogramowanie.
2. Obecna liczba stanowisk: 1170
3. Docelowa liczba stanowisk: 1200

II. Wymagania techniczne

1. Administracja zdalna
 - a. 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.
 - b. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
 - c. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
 - d. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
 - e. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
 - f. 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.
 - g. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
 - h. 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).
 - i. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.



- j. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
- k. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
- l. 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.
- m. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
- n. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
- o. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

2. Ochrona stacji roboczych

- a. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
- b. Rozwiązanie musi wspierać architekturę ARM64.
- c. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
- d. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
- e. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
- f. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
- g. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
- h. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
- i. 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.
- j. 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).
- k. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
- l. 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.
- m. 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.
- n. 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.
- o. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
- tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - 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,
 - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
- p. 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.
- q. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
- r. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- s. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antyvirus, antyspyware, metody heurystyczne).
- t. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- u. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego MS Outlook.
- v. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
- tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
 - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
- w. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
- x. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.



- y. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
- z. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
 - aa. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
 - bb. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
 - cc. 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.

3. Ochrona serwera

- a. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
- b. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
- c. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
- d. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
- e. 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.
- f. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- g. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
- h. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
- i. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
- j. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
- k. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
- l. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- m. 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 USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
- n. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
- o. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.



- p. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
- q. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

- r. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
- s. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
- t. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
- u. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszzonego mikro-serwisu.

4. Szyfrowanie

- a. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
- b. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
- c. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
- d. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

5. Ochrona urządzeń mobilnych opartych o system Android

- a. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
- b. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
- c. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
- d. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
- e. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
 - o nazwę aplikacji,
 - o nazwę pakietu,
 - o kategorię sklepu Google Play,
 - o uprawnienia aplikacji,
 - o pochodzenie aplikacji z nieznanego źródła.