

## Szczegółowy opis przedmiotu zamówienia

### I. Przedmiot zamówienia.

1. Przedmiotem jest dostawa na rzecz Gminy Lublin kluczy licencyjnych umożliwiających subskrypcję pakietu ochrony antywirusowej stacji roboczych, serwerów i urządzeń mobilnych przed szkodliwym oprogramowaniem dla 13 100 urządzeń.
  - 1.1. Klucze licencyjne muszą umożliwiać ochronę antywirusową realizowaną za pomocą systemu informatycznego, który składa się z:
    - a) Konsoli – serwera lub serwerów zainstalowanych w zasobach Zamawiającego wraz z oprogramowaniem służącym do obsługi systemu oraz zarządzania nim przez administratorów.
    - b) Oprogramowania – oprogramowanie działające na Urządzeniach i świadczące usługi ochrony antywirusowej oraz komunikujące się z Konsolą.
    - c) Elementów pośredniczących – proxy, relay; jeśli System wymaga ich do komunikacji. Zamawiający dopuszcza rozwiązanie chmurowe elementów pośredniczących pod warunkiem pisemnego poświadczenia przez producenta rozwiązania, że zasoby te znajdują się na terenie Unii Europejskiej.
    - d) Dodatkowego serwera pośredniczącego – dedykowanego dla izolowanych sieci Zamawiającego.
    - e) Licencji i subskrypcji – zapewnione przez Wykonawcę.

### II. Realizacja przedmiotu zamówienia.

1. W ramach realizacji przedmiotu zamówienia Wykonawca:
  - 1.1. Przeprowadzi analizę przedwdrożeniową uwzględniającą:
    - a) Architekturę rozwiązania i mechanizmy komunikacji Konsoli z serwerami pośredniczącymi i Urządzeniami.
    - b) Istniejącą strukturę Urządzeń objętych wdrożeniem.
    - c) Scenariusze tworzenia i odzyskiwania kopii zapasowych.
    - d) Ustalenie adresacji sieciowej wszystkich komponentów i zasady konfiguracji firewalli Zamawiającego.
    - e) Przygotowanie do akceptacji przez Zamawiającego harmonogramu obejmującego Konsolę Systemu, instalację oprogramowania na Urządzeniach w liczbie 1000 sztuk oraz wykonanie testów odbiorowych. Zamawiający wskaże do 10 lokalizacji, w których zostanie przeprowadzona instalacja oprogramowania na Urządzeniach. Harmonogram musi uwzględniać lokalizacje, terminy oraz liczbę Urządzeń podlegających wdrożeniu.
    - f) Przedłożona dokumentacja przedwdrożeniowa musi uzyskać akceptację Zamawiającego.
  - 1.2. Udostępni oprogramowanie w Centralnej Konsoli (Konsoli) i skonfiguruje je w infrastrukturze Zamawiającego.
  - 1.3. Uruchomi niezbędne komponenty umożliwiające funkcjonowanie Usługi na 1 000 Urządzeniach wskazanych przez Zamawiającego wraz z integracją z Centralną Konsolą (pozostałe Urządzenia Zamawiający skonfiguruje samodzielnie).
2. Dzięki dostarczonej licencji w Konsoli będzie możliwe połączenie i synchronizacja z minimum 3 Kontrolerami Domeny posiadanymi przez Zamawiającego. W wyniku wykonanej synchronizacji zostanie odtworzona struktura architektury drzewa w Konsoli (architektura drzewa).
3. Zamawiający przewiduje objęcie ochroną następujące rodzaje urządzeń:
  - 3.1. Stacje robocze (zestawy stacjonarne i laptopy) – 12 000 szt.

- 3.2. Urządzenia mobilne – do 1 000 szt.
- 3.3. Serwery – do 100 szt.
- 4. Sumaryczna liczba Urządzeń objętych ochroną przez cały okres obowiązywania Umowy wyniesie 13 100 sztuk.

### **Niezbędne zasoby i instruktaże**

#### **III. Zasoby Zamawiającego.**

Na potrzeby realizacji zamówienia Zamawiający dedykuje zasoby do osadzenia Konsoli wraz z niezbędnymi elementami:

- a) 8 vCPU Intel Xeon E5-2650;
- b) 16 GB RAM;
- c) przestrzeń dyskowa 300GB;
- d) system operacyjny bazujący na posiadanej przez Zamawiającego licencji Microsoft Windows co najmniej 2016 R2 Data Center lub 2019 Data Center;
- e) system operacyjny Linux w dowolnej dystrybucji wspieranej przez VMware;
- f) dostęp do Konsoli Systemu poprzez VPN dla osób wskazanych i upoważnionych przez Wykonawcę;

Zamawiający używa systemów archiwizacji danych Avamar i DataDomain.

#### **IV. Licencje.**

Wykonawca zagwarantuje:

- 1. Wszystkie licencje niezbędne do poprawnego funkcjonowania Konsoli Systemu, potwierdzone dokumentem licencyjnym wystawionym przez producenta Systemu uprawniającym Zamawiającego do korzystania z Systemu.
- 2. Subskrypcje na Urządzenia, potwierdzone statusem licencji z Konsoli systemu.
- 3. Dopuszcza się nieograniczone licencjonowanie wieczyste/perpetual/enterprise.
- 4. W ramach systemu pracować będzie do 10 administratorów.

#### **V. Instruktaże.**

- 1. Zamawiający wymaga przeprowadzenia instruktaży dla administratorów Systemu – w liczbie do 10 osób.
- 2. Zakres szkolenia będzie obejmował co najmniej zaawansowany instruktaż stanowiskowy, przeprowadzony w siedzibie Zamawiającego lub w lokalizacji zapewnionej przez Wykonawcę, obejmujący instruktaż podstawowy z obsługi i zarządzania końcówką kliencką zainstalowaną na urządzeniach oraz instruktaż z zakresu niezbędnych funkcjonalności zapewniających sprawne zarządzanie środowiskiem skonfigurowanym do obsługi wielu jednostek Gminy Lublin, nadawania/odbierania uprawnień, tworzenia polityk, raportów, procedur bezpieczeństwa i zasad bezpiecznej eksploatacji, sposobów analizy logów, debugowania systemu.
- 3. Instruktaż dla administratorów Systemu wykonany będzie przez certyfikowanego trenera zakończony wydaniem certyfikatu ukończenia instruktażu. Zamawiający nie dopuszcza instruktażu online. Wykonawca ponosi koszty organizacji instruktażu

#### **VI. Testy odbiorowe.**

- 1. Wykonawca wykona testy Systemu obejmujące co najmniej:
  - 1.1. Centralną Konsolę systemu.
  - 1.2. Poprawność działania oprogramowania na Urządzeniach.
  - 1.3. Przeprowadzenie backupu i odtwarzania Konsoli systemu wraz ze skonfigurowaniem stałego, dziennego backupu niezbędnego do odtworzenia poprawnego działania Systemu.
  - 1.4. Gromadzenia i odczytywania logów systemu za pomocą oprogramowania Zamawiającego (Splunk).
- 2. Testy kończą się pełnym raportem z przeprowadzonych czynności.

ZP-P-I.271.93.2025	Załącznik nr 1 do SWZ - Szczegółowy opis przedmiotu zamówienia	Str. 2 z 5
--------------------	--	------------

- 2.1. Opracowanie dokumentacji powykonawczej w języku polskim obejmującej co najmniej:
  - a) architekturę systemu wraz z opisem,
  - b) opis komponentów Systemu,
  - c) zasady bezpieczeństwa komunikacji, w szczególności bezpieczną komunikację stacji roboczych i serwerów poprzez wyłącznie szyfrowane połączenia i uwierzytelnienia poprzez architekturę certyfikatów SSL,
  - d) dokumentację dla administratorów Systemu,
  - e) wynik z przeprowadzenia backup i odtworzenia.
  - f) raporty z wdrożenia zawierające raporty z przeprowadzonego instruktażu.

### **Opis właściwości systemu informatycznego**

#### **VII. Właściwości systemu informatycznego.**

1. System musi zapewniać poufność, a wymiana danych z oprogramowaniem musi odbywać się w kanale szyfrowanym (SSL).
2. System musi zapewniać komunikację pomiędzy Konsolą a Urządzeniami również poprzez połączenia NAT, bez potrzeby korzystania z technologii VPN.
3. Dystrybucja oprogramowania musi być realizowana każdą z poniższych metod:
  - 3.1. poprzez instalację oprogramowania z poziomu Konsoli programu w przypadku integracji systemu z usługą Active Directory;
  - 3.2. poprzez instalację oprogramowania za pomocą reguł GPO; Zamawiający preferuje pakiety MSI generowany wprost z Konsoli;
  - 3.3. poprzez wysłanie linku do pobrania oprogramowania dedykowanego dla danej grupy Urządzeń;
  - 3.4. za pomocą dedykowanej paczki instalacyjnej dla co najmniej jednostki organizacyjnej Gminy reprezentowanej w drzewie architektury w Konsoli.

#### **VIII. Właściwości Konsoli.**

1. Architektura Konsoli musi być jednoinstancyjna, tzn. zapewniać dostęp do wszystkich zarządzanych przez system Urządzeń w ramach pojedynczej, zintegrowanej Konsoli administratorskiej (bez wymuszonego podziału na funkcjonalnie podobne podsystemy celem obsługi wszystkich objętych licencjonowaniem Urządzeń).
2. Zamawiający dopuszcza możliwości korzystania z komercyjnego silnika bazy danych w przypadku, gdy jego instancja będzie dedykowana tylko na potrzeby wdrożenia, bez ponoszenia dodatkowych kosztów przez Zamawiającego. Zapewnienie właściwych licencji bazodanowych jest w takim przypadku obowiązkiem Wykonawcy.
3. Interfejs Konsoli musi być w całości dostępny z poziomu przeglądarki internetowej (Mozilla, Chrome, Edge w najnowszych i dwóch wersjach wstecz) bez potrzeby instalacji dedykowanego klienta. Dostęp do Konsoli nie może wymagać korzystania z wtyczek w technologii Flash lub Java. Rekomenduje się wykorzystanie otwartej technologii HTML5.
4. Interfejs Konsoli musi być co najmniej w języku polskim lub angielskim.
5. Obsługa Konsoli musi umożliwiać zmianę kontrastu wyświetlanego obrazu oraz wielkość stosowanych czcionek ekranowych, co najmniej poprzez zmianę ustawień przeglądarki internetowej.
6. Konsola musi eksportować swoje logi w standardzie syslog. Zamawiający preferuje wykorzystanie modułu komunikacji z systemem Splunk.
7. Konsola musi zapewniać równoczesny, nieograniczony dostęp do Konsoli dla co najmniej 10 administratorów.
8. Konsola musi rozpoznawać Urządzenia z systemem Microsoft Windows w ramach Active Directory oraz Grup roboczych będących w posiadaniu Zamawiającego, w tym środowiska wielodomenowego.

9. Konsola musi zapewniać drzewiastą i hierarchiczną architekturę dla jednostek, administratorów i Urzędzeń.
10. Konsola musi zapewniać delegację uprawnień do określonych grup zasobów na podstawie uprzednio zdefiniowanych reguł. Wśród dostępnych reguł i uprawnień muszą znajdować się co najmniej:
  - 10.1. tworzenie użytkowników Konsoli,
  - 10.2. usuwanie użytkowników Konsoli,
  - 10.3. edycja użytkowników Konsoli,
  - 10.4. nadawanie dostępu do gałęzi drzewa architektury dla użytkowników Konsoli,
  - 10.5. odbieranie dostępu do gałęzi drzewa architektury dla użytkowników Konsoli,
  - 10.6. zarządzanie użytkownikami, ich uprawnieniami i przypisywanie im ról (w tym poziomów uprawnień dla administratorów), a także zarządzanie rolami musi odbywać się poprzez interfejs Konsoli, przypisywanie uprawnień może odbywać się na podstawie przynależności użytkownika do odpowiedniej grupy w Active Directory,
  - 10.7. tworzenie ról użytkowników,
  - 10.8. usuwanie ról użytkowników,
  - 10.9. modyfikowanie ról użytkowników,
  - 10.10. dodawanie Urzędzeń,
  - 10.11. usuwanie Urzędzeń,
  - 10.12. definiowanie zadań,
  - 10.13. uruchamianie zadań,
  - 10.14. tworzenie i edycja polityk.
11. Konsola musi zapewniać uwierzytelnianie Administratorów na podstawie członkostwa do wcześniej zdefiniowanej Grupy Zabezpieczeń (Security Group) w Active Directory.
12. Konsola musi umożliwiać tworzenie raportów (zdefiniowanych przez Producenta oprogramowania oraz niestandardowych) na podstawie wbudowanych kryteriów, w tym na podstawie podziału na jednostki. Poza standardowymi (wbudowanymi) raportami, System musi generować następujące rodzaje raportów:
  - 12.1. Cykliczny (miesięczny) raport z wykorzystania licencji z podziałem na Jednostkę, ilość wykorzystanych licencji i datę ostatniej aktywności Urzędzenia.
  - 12.2. Cykliczny (miesięczny) raport z wykorzystania licencji z podziałem na Jednostkę, ilość wykorzystanych licencji i datę ostatniej aktywności Urzędzenia prezentowany również w formie graficznej.
  - 12.3. Sumaryczny raport wszystkich Urzędzeń w Konsoli z podziałem na rodzaj Urzędzenia, tj. serwery, stacje robocze, urządzenia mobilne oraz ich systemy operacyjne wraz z datą ostatniej aktywności Urzędzenia.
  - 12.4. Wykaz administratorów wraz przypisanymi Jednostkami oraz ich rolami w Systemie oraz datę ostatniej aktywności w konsoli.
13. Konsola musi mieć możliwość włączenia opcji testowania i zatwierdzania aktualizacji na wybranej grupie urządzeń przed instalacją poprawek w środowisku produkcyjnym.
14. Administrator Konsoli musi mieć możliwość pobrania dedykowanej paczki instalacyjnej z poziomu Konsoli.
15. Konsola musi umożliwiać zarządzanie i rozliczanie licencji oprogramowania.
16. Konsola musi umożliwiać zdalne wykrywanie zainfekowanego oprogramowania i uruchamiać zdefiniowane działania naprawcze.
17. Konsola musi zapewniać poprawną obsługę oprogramowania w przypadku, gdy nazwy Urzędzeń i ich adresacja w różnych sieciach powtarzają się.
18. Konsola musi posiadać wbudowane narzędzia systemowe umożliwiające wymuszenie zdalnej aktualizacji na wskazanych Urzędzeniach oraz zarządzanie harmonogramami skanowania.

19. Konsola musi umożliwiać wykonywanie zadań w określonym przedziale czasowym oraz wysyłać powiadomienia e-mail o zmianach, które wystąpiły w systemie.
  20. Konsola musi umożliwiać tworzenie harmonogramów dla raportów i przysyłanie ich w formie pliku XLSX lub CSV lub ODS na wskazany adres mailowy oraz udostępniać możliwość zapisania raportu lokalnie.
  21. Konsola musi zapewniać na tworzenie dedykowanej paczki instalacyjnej, po zainstalowaniu której umożliwi jednoznaczną identyfikację Urzędzeń w drzewie architektury.
- IX. Właściwości oprogramowania na Urzędzeniach.
1. Interfejs oprogramowania musi być dostępny w języku polskim na Urzędzeniach.
  2. Oprogramowanie na Urzędzeniach musi działać nawet w przypadku utraty łączności z Konsolą systemu.
  3. Urządzenia muszą samodzielnie aktualizować sygnatury antywirusowe w przypadku utraty komunikacji z Konsolą systemu.
  4. Oprogramowanie stacji roboczych musi obsługiwać systemy operacyjne będące w posiadaniu Zamawiającego lub użytkowane przez jednostki Gminy Lublin w wersjach:
    - 4.1. Microsoft Windows 10, 11 i nowszych.
    - 4.2. Linux Debian 10.x, Ubuntu 20.x i nowszych.
    - 4.3. MacOS 13.xi nowszych.
  5. Oprogramowanie urządzeń mobilnych musi obsługiwać systemy operacyjne będące w posiadaniu Zamawiającego lub użytkowane przez jednostki Gminy Lublin w wersjach:
    - 5.1. iOS.
    - 5.2. Google Android.

Dopuszczalne jest zaoferowanie Konsoli chmurowej tego samego producenta jedynie dla urządzeń mobilnych.
  6. Oprogramowanie serwerowe musi obsługiwać systemy operacyjne będące w posiadaniu Zamawiającego lub użytkowane przez jednostki Gminy Lublin w wersjach:
    - 6.1. Microsoft Windows 2012 Data Center i nowsze.
    - 6.2. Linux Debian 10.x, Ubuntu 20.x, i nowsze.
  7. Oprogramowanie na Urzędzeniach musi zapewniać automatyczne skanowanie pod kątem zagrożeń i ewentualne blokowanie urządzeń i nośników wymiennych (karty pamięci, urządzenia USB) w przypadku wykrycia zagrożenia.
  8. Oprogramowanie na Urzędzeniach musi zapewniać automatyczną deinstalację innego oprogramowania antywirusowego podczas instalacji.
  9. Oprogramowanie na Urzędzeniach musi mieć wbudowane narzędzie informujące o brakujących aktualizacjach systemowych.
  10. Oprogramowanie na stacjach roboczych musi gwarantować minimalne wyniki dla co najmniej jednego ze wskazanych poniżej testów oferowanego oprogramowania przeprowadzonych przez jeden z niezależnych ośrodków dla sektora Enterprise w kategorii ochrony dla komputerów stacjonarnych z systemem Windows na poziomie:
    - 10.1. Odpowiedni wynik w teście Windows AV-TEST antivirus software for business users w kategorii Protection - ocena min. 6.
    - 10.2. Odpowiedni wynik w teście AV-Comparatives Real-World Protection Test - min. 99%.
    - 10.3. Odpowiedni wynik w teście SELabs Security Evaluation Test Report: Enterprise End-point Security (Protection) - min. 99%.