



Część II SWZ
Zamówienie Częściowe nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa i wdrożenie systemu kontroli danych (DLP)

I. Przedmiot zamówienia

W związku z rozbudową systemów bezpieczeństwa Urzędu Miasta Gorzowa Wlkp., Zamawiający zamierza wdrożyć system DLP (Data Loss Prevention).

Przedmiotem zamówienia jest dostawa, instalacja, zaawansowana konfiguracja oraz szkolenia personelu w zakresie systemu DLP.

II. Wymagania funkcjonalne systemu

1. Przedmiot umowy musi być dostarczony z licencją bezterminową wraz ze wsparciem produktowym producenta przez okres minimum 24 miesięcy (upgrade do najnowszej wersji, pomoc techniczna).
2. System musi być dostarczony w najnowszej dostępnej wersji oprogramowania.
3. Oferowane oprogramowanie musi posiadać wsparcie, którego co najmniej pierwsza linia jest świadczona w języku polskim.
4. System operacyjny:
 - a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi,
 - b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi,
 - c. MacOS 12 lub nowszy.
5. Serwer administracyjny musi obsługiwać instalację na systemach Windows Server 2016 (64-bit) i nowszych.
6. Serwer administracyjny musi obsługiwać bazy danych:
 - a. MS SQL Server 2016 lub nowsze,
 - b. MS SQL Express,
 - c. AzureSQL S3 lub nowsze.
7. Pomoc i dokumentacja programu dostępne w języku angielskim.
8. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
9. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
10. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.
11. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem, a serwerem zarządzającym.
12. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
13. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.



14. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.
15. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
16. Administrator musi mieć możliwość, aby tworzyć, usuwać i konta administratorów w konsoli programu.
17. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
18. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
19. System musi rejestrować zdarzenia aktywności stacji roboczej, takie jak logowanie, wylogowanie, włączenie, wyłączenie, blokada, odblokowanie i przejście w stan bezczynności.
20. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą, a serwerem w czasie rzeczywistym.
21. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
22. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości e-mail oraz czynności na plikach.
23. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
24. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
25. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
26. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
27. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.
28. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
29. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
30. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych, jak i sieciowych.
31. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.



32. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.
33. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
34. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
35. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
36. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
37. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysłaną przez użytkowników Microsoft 365.
38. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
39. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach.

III. Wymagania wdrożeniowe

1. Opracowanie harmonogramu wdrożenia systemu DLP.
2. Przeprowadzenie przez Wykonawcę analizy przedwdrożeniowej oraz przygotowanie projektu technicznego wdrożenia.
3. Przeprowadzenie instalacji i konfiguracji systemu DLP.
4. Przygotowanie i przeprowadzenie scenariuszy testowych weryfikujących wydajność i poprawność wdrożonego systemu w środowisku Zamawiającego.
5. Uzyskanie akceptacji Zamawiającego dla proponowanych scenariuszy.

IV. Wymagania w zakresie szkoleń

1. Wykonawca dostarczy voucher szkoleniowy dla dwóch słuchaczy dla systemu DLP.
2. Szkolenie odbędzie się w formie zdalnej lub stacjonarnej.
3. Szkolenie musi być prowadzone w języku polskim.
4. Każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim lub angielskim.
5. Osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania potwierdzający ich kompetencje w zakresie użytkowania i administrowania systemem.