



Opis przedmiotu zamówienia

Oprogramowanie zapewniające poufny danym ochronę przed ich udostępnieniem osobom nieupoważnionym, wykrywanie zagrożeń wewnętrznych i wczesne ograniczanie ryzyka wycieku poufnych danych 30 użytkowników – Urząd Gminy

Minimalne wymagania techniczne

1. System operacyjny:

- a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
- b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
- lub równoważne

2. Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 (64-bit) i nowszych. – lub równoważne

3. Serwer administracyjny musi obsługiwać bazy danych: a. MS SQL Server 2016 lub nowsze, b. MS SQL Express, c. AzureSQL S3 lub nowsze. – lub równoważne

4. Pomoc i dokumentacja programu dostępne w języku angielskim.

5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.

6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.

7. Serwer administracyjny musi umożliwiać instalację/deinstalację zdalnego klienta na stacjach roboczych.

8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.

9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.

10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.



- 11.** Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.
- 12.** Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
- 13.** Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
- 14.** Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
- 15.** Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
- 16.** System musi rejestrować zdarzenia aktywności stacji roboczej, takie jak logowanie, wylogowanie, włączenie, wyłączenie, blokada, odblokowanie i przejście w stan bezczynności.
- 17.** Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
- 18.** 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.
- 19.** 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 email oraz czynności na plikach.
- 20.** Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
- 21.** Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
- 22.** Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
- 23.** Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.



- 24.** Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.
- 25.** 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.
- 26.** Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
- 27.** Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych, jak i sieciowych.
- 28.** 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.
- 29.** 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.
- 30.** Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
- 31.** Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
- 32.** Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
- 33.** Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
- 34.** System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysłaną przez użytkowników Microsoft 365. – lub równoważne
- 35.** System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams. – lub równoważne



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- 36.** System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach
- 37.** Minimalna ilość wymaganych licencji nie może być mniejsza niż 180.
- 38.** Okres ważności licencji – bezterminowe
- 39.** Okres ważności wsparcia producenta – co najmniej 12 miesięcy