Załącznik nr 1 do SWZ

Nr postępowania: WIR.271.5.2025

**OPIS PRZEDMIOTU ZAMÓWIENIA – Zadanie 3 obszar techniczny**

**Pozycja 8. SYSTEMU DLP - DATA LOSS PREVENTION zakup wraz z wdrożeniem – 1 kpl.**

MINIAMALNE WYMAGANIA SYSTEMOWE

1. System operacyjny:
   1. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
   2. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
   3. MacOS 12 lub nowszy.
2. Serwer administracyjny musi obsługiwać instalację na systemach:
   1. Windows Server 2016 (64-bit) i nowszych.
3. Serwer administracyjny musi obsługiwać bazy danych:
   1. MS SQL Server 2016 lub nowsze,
   2. MS SQL Express,
   3. AzureSQL S3 lub nowsze.

KOMUNIKACJA I JĘZYK

1. Pomoc i dokumentacja programu dostępne w języku angielskim.
2. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.

FUNKCJONALNOŚCI ZARZĄDZANIA

1. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
2. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.
3. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
4. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
5. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
6. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
7. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.

KONTROLA I ZARZĄDZANIE DANYMI

1. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
2. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
3. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.
4. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.

BEZPIECZEŃSTWO I MONITORING

1. 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.
2. 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.
3. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
4. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.
5. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.

KATEGORYZACJA I OCHRONA PLIKÓW

1. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
2. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
3. 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.
4. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
5. 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.
6. 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.
7. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.

INTEGRACJA I KONFIGURACJA

1. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
2. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
3. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.
4. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
5. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach.
6. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.)
7. System musi zapewniać możliwość zarządzanie szyfrowaniem dysków twardych oraz urządzeń wymiennych.

WDROŻENIE I WSPARCIE

1. Przed rozpoczęciem wdrożenia jeśli jest to wymagane Zleceniobiorca powinien przeprowadzić wstępne spotkanie, na którym zostaną omówione wszystkie kroki procesu wdrożeniowego
2. Przed docelowym uruchomieniem systemu zaleca się przeprowadzenie testów integracyjnych i akceptacyjnych, aby upewnić się, że wszystkie elementy systemu działają poprawnie i są zgodne z wymaganiami zleceniodawcy.
3. Przed pełnym uruchomieniem zrealizowane zostanie przeszkolenie pracowników z obsługi nowego systemu. Dostawca powinien zapewnić odpowiednie materiały szkoleniowe oraz warsztaty praktyczne.
4. Dostawca zobowiązany jest zapewnić ciągłe wsparcie techniczne w czasie pierwszych dni po wdrożeniu, aby szybko reagować na ewentualne problemy i pytania użytkowników końcowych.
5. Dostawca zobowiązany jest do zapewnienia kompleksowego wsparcia technicznego przez okres 24 miesięcy po wdrożeniu systemu. Wsparcie obejmuje zarówno pomoc zdalną, jak i możliwość interwencji serwisowych na miejscu w przypadku krytycznych awarii.
6. W ramach serwisu, dostawca gwarantuje regularne aktualizacje systemu, które będą obejmować zarówno nowe funkcjonalności, jak i łatki bezpieczeństwa.