Załącznik Nr 6

System klasy DLP – system do ochrony danych przed wyciekiem danych

Opis przedmiotu szacowania:

Przedmiotem zamówienia jest dostawa systemu ochrony przed wyciekiem informacji DLP (Data Loss Prevention), wraz z kompletem niezbędnych licencji, przeszkoleniem pracowników oraz zapewnieniem wsparcia technicznego i serwisu dla zaoferowanego systemu.

1. Pełne wsparcie dla systemów operacyjnych:
   1) Windows 10 (64-bit).
   2) Windows 11 (64-bit).
2. Serwer administracyjny musi obsługiwać instalację na systemach: Windows Server 2016 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.
4. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
5. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
6. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.
7. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
8. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
9. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
10. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.
11. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
12. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
13. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
14. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
15. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
16. 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.
17. 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.
18. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
19. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
20. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
21. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
22. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.
23. 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.
24. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
25. 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.
26. 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.

27. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
28. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
29. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
30. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
31. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.
32. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
33. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach.
34. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.)
35. System musi zapewniać możliwość zarządzania szyfrowaniem dysków twardych oraz urządzeń wymiennych.
36. Dostawa niezbędnych licencji i oprogramowania oferowanego systemu DLP dla 60 stanowisk.
37. System musi posiadać aktywne wsparcie producenta w okresie 24 miesięcy od daty podpisania bez uwag protokołu odbioru, umożliwiające aktualizację do najnowszych wersji oraz wsparcie Wykonawcy w zakresie zgłaszania w dni robocze ewentualnych problemów drogą mailową, przez portal online oraz telefonicznie, w godzinach 8:00 – 15:00.
38. Świadczenie serwisu i wsparcia technicznego wykonawcy przez okres 24 miesięcy liczonego.
39. Wykonawca zapewni szkolenie w zakresie użytkowania i administrowania wdrożonego systemu. Szkolenie ma zostać przeprowadzone dla 1 osoby i musi być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez producenta systemu. Szkolenia mogą odbyć się w formie zdalnej.