

Załącznik nr 3

SZCZEGÓŁOWY FORMULARZ OFERTOWY

Nazwa

oprogramowania:.....

Producent:.....

.....

Lp.	Zakres wymagań	Wymagania minimalne	Tak/ Nie*
1	Podstawowe wymagania techniczne i technologiczne dla rozwiązania	1. System musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.	Tak/ Nie
		2. Komponenty oprogramowania instalowane na stacjach użytkowników muszą być zgodne z systemem operacyjnym Windows 10 i zapewniać wsparcie dla 32 i 64-bitowej wersji systemu Windows.	Tak/ Nie
		3. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server, 2016, 2019.	Tak/ Nie
		4. Administrator musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z usługą Active Directory.	Tak/ Nie
		5. System musi zapewniać ochronę urządzenia końcowego bez względu na to, czy komputer jest podłączony do sieci czy nie.	Tak/ Nie
		6. System musi umożliwiać zarządzanie za pośrednictwem konsoli webowej	Tak/ Nie
		7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta, a serwer administracyjny musi umożliwiać wykonanie instalacji/deinstalacji zdalnej klienta na stacjach roboczych. Agent musi być zabezpieczony przed wyłączeniem i restartem przez użytkownika.	Tak/ Nie
		8. Rozwiązanie musi reagować na próby wysyłania poufnych danych z i na urządzenia końcowe, musi zapewniać ochronę nawet, gdy urządzenie nie jest podłączone do sieci korporacyjnej. Rozwiązanie musi monitorować co najmniej wysyłane wiadomości email, HTTP/HTTPS, FTP, kopiowanie danych z komputera na udział sieciowy, kopiowanie danych z udziału sieciowego do komputera przez Windows Explorer, SFTP, SSH, Bluetooth, Skype, WebEx, LiveMeeting i inne. Musi blokować użycie i wysyłkę poufnych danych przez dowolną aplikację. Musi	Tak/ Nie

		monitorować i blokować kopiowanie danych na przenośne urządzenia (USB, CD/DVD, SD/CF, eSATA itp) pozwalając jednocześnie na kopiowanie informacji na zaakceptowane urządzenia przenośne. Rozwiązanie musi monitorować i blokować próby drukowania bądź faksowania zabezpieczonych danych.	
		9. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu , a rozwiązanie musi pozwalać na stosowanie różnych polityk dla różnych urządzeń końcowych i użytkowników. Rozwiązanie musi rozróżniać polityki dla dwóch różnych użytkowników zalogowanych na tym samym komputerze.	Tak/ Nie
		10. Rozwiązanie musi umożliwiać tagowanie plików na poziomie systemu plików lub na poziomie metadanych pliku - zarówno plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, jak i nowych plików, które powstaną na bazie istniejących plików z tagami.	Tak/ Nie
		11. System musi posiadać możliwość zaszyfrowania całej powierzchni dysku i dysków zewnętrznych. Musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych. Dla zaszyfrowanych dysków zewnętrznych czy pamięci typu pendrive, musi być możliwość uruchomienia i dostępu do danych poza strukturą Zamawiającego, np. poprzez podanie hasła.	Tak/ Nie
		12. Rozwiązanie musi mieć możliwość ustawień powiadomień do użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ustawieniami DLP. Jednocześnie musi istnieć możliwość wycofania funkcji blokującej przez administratora lub osobę wyznaczoną.	Tak/ Nie
		13. System musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączone urządzenia, odwiedzone strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.	Tak/ Nie
		14. Dostarczony system musi umożliwić objęcie ochroną min. 300 urządzeń (lub 250 użytkowników – w zależności od zasad licencjonowania). Dostarczona licencja musi być bezterminowa.	Tak/ Nie
	Dodatkowe wymagania	Wymaganie dodatkowe (dodatkowo punktowane) - Konsola administracyjna oraz komunikaty klienta w języku polskim.	Tak/ Nie

* Niepotrzebne skreślić

