Załącznik Nr 4

SZCZEGÓŁOWY OPIS PRZEDMOTU ZAMÓWIENIA

1. **Postanowienia ogólne.**
2. **Oprogramowanie antywirusowe – 1 szt.**
3. **System DLP – 1 szt.**

1. Postanowienia ogólne.

Przedmiotem zamówienia jest zakup i dostawa oprogramowania dla Ośrodka Pomocy Społecznej w Czerwionce-Leszczynach.

Zakres przedmiotu umowy obejmuje dostawę:

1) oprogramowania antywirusowego – 1 szt (ochrona 85 stacji roboczych),
2) systemu DLP – 1 szt (ochrona 100 stacji roboczych),

spełniających wszystkie parametry techniczne - wymagania minimalne Zamawiającego określone w niniejszym Szczegółowym Opisie Przedmiotu Zamówienia.

2. Oprogramowanie antywirusowe – 1 szt.

Lp.	Parametry techniczne - wymagania minimalne
1	Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2	Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3	Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4	Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5	Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6	Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM
7	Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8	Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9	Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10	Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11	Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera
12	Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo,

	comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
13	Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
14	Rozwiązanie musi wspierać architekturę ARM64.
15	Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
16	Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
17	Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
18	Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
19	Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
20	Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
21	Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
22	Rozwiązanie musi integrować się z Intel Threat Detection Technology.
23	Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
24	Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
25	Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

26	Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
27	Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
28	Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
29	Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
30	Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
31	Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

32	Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
33	Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
34	Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
35	Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: • tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, • tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
36	Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
37	Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
38	Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
39	Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
40	Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
41	Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
42	W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

43	Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
44	Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
45	Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
46	Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
47	Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
48	Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
49	Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
50	Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
51	Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
52	Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
53	Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
54	Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
55	Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych

	pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
56	Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
57	Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
58	Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
59	Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
60	Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
61	Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
62	System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
63	System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
64	Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
65	Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
66	Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
67	Rozwiązanie musi wykorzystywać do działania chmurę producenta.
68	Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.

69	Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
70	Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
71	Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
72	Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
73	Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
74	Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
75	Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
76	Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
77	Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: a)Czysty, b)Podejrzany, c)Bardzo podejrzany, d)Szkodliwy.
78	W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

79	W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
80	Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.
	Moduł XDR oprogramowania antywirusowego
81	Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
82	Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
83	Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
84	Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
85	Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
86	Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
87	Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
88	Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
89	Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
90	Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
91	Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia.

92	Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
93	W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
94	W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
95	Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
96	Konsola administracyjna musi mieć możliwość tagowania obiektów.
97	Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
98	Licencja musi umożliwiać równoległa ochronę dla co najmniej 85 stacji roboczych
99	Wsparcie producenta i czas trwania licencji na okres minimum 12 miesięcy.

3. System DLP – 1 szt.

Lp.	Parametry techniczne - wymagania minimalne
1	Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10/Windows11.
2	Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 (64-bit) i nowszych.
3	Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim.
4	Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
5	Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL oraz AzureSQL.
6	Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.
7	Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
8	Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.
9	Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem, a serwerem zarządzającym.
10	W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.
11	Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.
12	Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania: kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z

	wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.
13	Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.
14	Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania oraz edycji wyżej wymienionych kategorii.
15	Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania.
16	Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na: • Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module, • Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.
17	Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory.
18	System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej: a) logowanie oraz wylogowanie użytkownika, b) włączenie oraz wyłączenie stacji roboczej, c) blokada oraz odblokowanie stacji roboczej, d) przejście w stan bezczynności stacji roboczej.
19	Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym.
20	Serwer administracyjny musi mieć możliwość ustawienia powiadomień dla użytkownika

	końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji.
21	Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.
22	Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików.
23	Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF oraz XLS.
24	Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
25	Serwer musi posiadać możliwość wysłania alertów, co najmniej za pośrednictwem wiadomości email.
26	Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.
27	Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
28	Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail.
29	Serwer administracyjny musi posiadać domyślnie skonfigurowany serwer SMTP udostępniony przez producenta oprogramowania.
30	Serwer administracyjny musi umożliwiać kategoryzację (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku.

31	Serwer administracyjny musi umożliwiać wykonanie zadania kategoryzacji (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie już skategoryzowanych (otagowanych) plików.
32	Serwer administracyjny musi mieć możliwość kategoryzacji (tagowania) plików wrażliwych w oparciu o: a) aplikacje, z której zostały utworzone, b) lokalizację, c) adres URL, d) format pliku, e) zawartość pliku.
33	Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych jak i sieciowych.
34	Dla plików skategoryzowanych (otagowanych), musi być możliwe utworzenie następujących reguł: a) blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych, b) blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń, c) blokowanie oraz zezwalanie na drukowanie na określonych drukarkach, d) blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej, e) blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen, f) blokowanie oraz zezwalanie na wysyłanie do poczty webowej, g) blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi: • Dropbox,

	• Google Drive, • SharePoint, • OneDrive Business, • OneDrive Personal. h) blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów, i) blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego, j) blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości oraz wirtualnego drukowania, k) uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje,
35	Serwer administracyjny musi umożliwiać możliwość zabezpieczenia korzystania z niezaufanych repozytoriów GIT.
36	Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.
37	Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.
38	Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę klasyfikacji na niższą.
39	Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających urządzenia pamięci masowej, drukarki fizycznych i sieciowych, lokalizacji sieciowych, adresów e-mail oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu.
40	Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury.

41	Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.
42	Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
43	Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika.
44	Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych.
45	Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o: a) numery kart kredytowych, b) numer PESEL, c) numer polskiego dowodu osobistego, d) polski numer paszportu, e) wyrażenia regularne, f) określone ciągi znaków, g) numer IBAN.
46	Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
47	Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition) z wsparciem języka polskiego.
48	System musi posiadać możliwość importu własnych słowników do wyszukiwania danych.
49	W przypadku incydentu bezpieczeństwa, system musi wykonać duplikat pliku lub wiadomości e-mail, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy”).

50	Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie klasyfikacji (tagowania).
51	Serwer administracyjny musi posiadać możliwość integracji klasyfikacji danych, z modułem DLP dostępnym na rozwiązaniu FortiGate.
52	Serwer administracyjny musi umożliwiać eksport logów do rozwiązania FortiSIEM.
53	Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych plików do rozwiązania FortiMail, które będzie w stanie kontrolować przesyłanie tak oznaczonych plików.
54	Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na: a) audyt i logowanie wiadomości e-mail, b) audyt operacji na plikach Sharepoint Online.
55	System musi umożliwiać integrację z narzędziami analitycznymi tj. Power BI, Tabeau).
56	Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi.
57	Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na: a) Bezpieczeństwo danych: • Przegląd informacji o incydentach bezpieczeństwa. • Przegląd danych przychodzących. • Przegląd danych wychodzących. • Podłączane/odłączane urządzenia przenośne. b) Produktywność: • Przegląd informacji na temat produktywności użytkowników. • Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji. • Trendy. c) Eksploatacja sprzętu:

	• Przegląd informacji na temat eksploatacji sprzętu komputerowego. • Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery. • Eksploatacja drukarek. • Eksploatacji sieci.
58	Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.
59	Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.
60	Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje nt: • plików przenoszonych na nośniki USB i inne urządzenia przenośne, • plików przesłanych za pomocą wiadomości e-mail, • plików przesłanych za pomocą poczty webowej, • plików przesłanych do Internetu, • plików wysłanych za pomocą komunikatorów, • plików przesłanych na dyski chmurowe, • analiza sposobu korzystania z aplikacji, • analiza korzystania z Internetu, • analiza wykorzystania portali do poszukiwania pracy.
61	Konsola aplikacyjna musi umożliwiać możliwość konfiguracji podwójnej autoryzacji
62	Konsola aplikacyjna musi umożliwiać konfigurację dwóch języków dla mechanizmu OCR
63	W ramach dostawy oprogramowania Wykonawca przeprowadzi: analizę przedwdrożeniową, instalację i konfigurację systemu DLP, integrację systemu z Active Directory, wdrożenie agenta na przykładowych 5 stacjach wskazanych przez Zamawiającego, zaprojektowanie i wdrożenie polityk bezpieczeństwa DLP.
64	Licencja musi umożliwiać równoległą ochronę dla co najmniej 100 stacji roboczych
65	Wsparcie producenta i czas trwania licencji na okres minimum 12 miesięcy.

Wykonawca dostarczy dokumentację powykonawczą w zakresie wdrożonych systemów, ich konfiguracji oraz poświadczenia dostępowe.