OP.272.15.2024

Załącznik Nr 1c do SWZ -Szczegółowy opis przedmiotu zamówienia do części 3

Dostawa licencji systemu DLP (Data Leak Prevention) – 90 szt. licencji
do użytku dla 4 różnych jednostek Powiatu Augustowskiego:

1. Dla Starostwa Powiatowego w Augustowie – ilość licencji – 65 sztuk.
2. Dla Powiatowego Zarządu Dróg w Augustowie – ilość licencji - 10 sztuk.
3. Dla Zespołu Placówek Młodzieżowych w Augustowie – ilość licencji – 5 sztuk.
4. Dla Augustowskiego Centrum Edukacyjnego w Augustowie – ilość licencji – 10 sztuk.

****

I. Oferowane oprogramowanie powinno:

1) składać się z serwera zarządzającego z lokalną konsolą, obsługiwaną przez przeglądarkę internetową
2) oraz agentów, zgodnych z systemami operacyjnymi Windows 10 i nowszych, Microsoft Windows Server 2016 i nowszych
3) umożliwiać instalację serwera zarządzającego na 64-bitowych wersjach systemu operacyjnego Windows Server 2016 i nowszych wersjach,
4) działać w technologii bazodanowej, na niepłatnych wersjach serwerów bazodanowych, np. MS SQL Express, Postgres, Firebird, MariaDB itp.,
5) system powinien zapewniać ochronę dla urządzeń w sieci lokalnej, pracujących zdalnie w sieci Internet oraz w innych oddziałach połączonych z siecią Starostwa za pośrednictwem VPN,
6) umożliwiać kontrolowanie na komputerach co najmniej:
    a. Napędy dyskietek,
    b. Napędy CD/DVD,
    c. Dyski wymienne: nośniki flash, karty pamięci, pendrive itd.
    d. Dyski twarde wewnętrzne i zewnętrzne
    e. Dyski sieciowe
    f. Napędy udostępnione,
    g. Adaptery Wi-Fi i urządzenia Bluetooth
    h. Urządzenia pamięci masowej PCMCIA
    i. Aparaty cyfrowe / kamery internetowe / thunderbolt
    j. Drukarki (USB, lokalne, sieciowe i wirtualne)
7) zapewnić ochronę porów USB, FireWire, szeregowych i równoległych,
8) zapewnić kontrolę komunikacji sieciowej: Poczta: MAPI , SMTP/SMTPS, Portale społecznościowe: Facebook, Twitter, Google+, LinkedIn, Protokoły internetowe: HTTP/HTTPS, FTP/FTPS, Telnet, Torrent, Serwisy chmurowe: Dropbox, Google Drive, Microsoft OneDrive,
9) identyfikować i analizować co najmniej formaty plików:
    a. MS Office, OpenOffice, CSV, TXT, DBF, XML, Unicode

b. pliki MIME
c. archiwa: GZIP, RAR, ZIP, inne

10) identyfikować i analizować co najmniej następujące typy danych:
    a. pliki pakietu MS OFFICE
    b. pliki PDF, TXT, XML
    c. predefiniowane pliki multimedialne
    d. predefiniowane pliki MIME
    e. oraz inne dowolnie definiowane pliki,
11) umożliwiać kontrolę schowka, w tym:
    a. Operacje kopiowania/wklejania treści między aplikacjami
    b. Identyfikowanie typu danych: pliki, dane tekstowe, multimedia oraz inne
    c. Zrzuty ekranu (Print Screen i aplikacje innych firm)
12) zapewniać integrację z szyfrowaniem: Windows BitLocker, PGP, TrueCrypt, SafeDisk i inne.
13) umożliwiać filtrowanie treści, wykorzystując:
    a. Słowa kluczowe
    b. Lokalizacja i kanał transferu danych
    c. Zaawansowane wzorce wyrażeń regularnych
    d. Predefiniowane szablony wyrażeń regularnych (PESEL, NIP, numer dowodu osobistego, numer paszportu, numer karty kredytowej, numer konta bankowego, adres, numer prawa jazdy, data, adres e-mail, kod pocztowy, numer telefonu itd.)
    e. Słownik: Międzynarodowa Klasyfikacja Chorób i Procedur Medycznych ICD-9, ICD-10
    f. Słowniki słów kluczowych
    g. Atrybuty plików (nazwa, rozmiar, data/czas, szyfrowanie itd.)
14) zapewniać blokadę, kontrolę oraz monitoring urządzeń, a także peryferii w celu uniemożliwienia kradzieży danych, poprzez:
    a. Stosowanie ustawień globalnych praw do urządzeń, jednak z możliwością zdefiniowania dodatkowych reguły dotyczących wybranych grup urządzeń
    b. Ustalenie praw dla komputerów, z możliwością indywidualnego definiowania dla każdego komputera, w szczególności dla komputerów, które pełnią specjalną rolę w organizacji: np. serwerów czy też komputerów administratorów.
    c. Ustalenie praw dla grupy urządzeń, poprzez dowolne grupowane - możliwość zdefiniowania różnych praw dostępu dla wybranych obszarów działalności lub elementów struktury organizacyjnej.
    d. Powiadomienia administracyjne np. w formie e-mail, definiowalne dla odpowiednich polityk bezpieczeństwa.
    e. Monitoring i analizę aktywności użytkowników oraz urządzeń z możliwością eksportu danych do wybranych formatów,
    f. Ustalenie praw dla konkretnego użytkownika, prawa dostępu mogą być ustalone dla użytkownika niezależnie od urządzeń, z jakich korzysta czy też będzie korzystał w przyszłości.
    g. Ustalenie praw dla urządzenia - prawa mogą być ustalone dla konkretnego urządzenia w oparciu np. o numer seryjny, identyfikator dostawcy oraz identyfikator produktu. System powinien potrafić identyfikować także nośniki szyfrowane.
    h. Monitorowanie transferów lub prób transferów plików (dokumentów) na urządzenia pamięci USB powinny być rejestrowane, dzięki czemu system daje możliwość podjęcia odpowiedniego działania (np. blokowanie działania)

i. Kopie plików (dokumentów) - Pliki kopiowane na nośniki zewnętrzne mogą być
j. zapisywane w repozytorium, tak aby później podczas audytu mogły zostać zweryfikowane.
k. Dashboard - odpowiednia prezentacja graficzna poprzez zaawansowany dashboard, na którym znajduje się wiele widżetów, które można dowolnie konfigurować
l. Powiadomienia użytkownika - powiadomienia mogą być np. w formie wyskakujących okien (pop-up) i informować/ostrzegać o działaniach, które w konsekwencji mogą prowadzić do naruszeń bezpieczeństwa. Powinny być w pełni definiowalne.

15) Zapewniać ochronę danych w spoczynku, poprzez identyfikację miejsc składowania danych oraz klasyfikację znalezionych danych, wykorzystując np.:
    a. wyrażenia wykluczone - zdefiniowane mechanizmy analizy treści lub zdefiniowane samodzielnie algorytmy do zbudowania statycznych czarnych list (black list),
    b. tzw. białe listy plików – definiowane w oparciu o szablon nazwy, rozszerzenie, rozmiar, datę utworzenia. Takie pliki nie będą podlegać skanowaniu i nie będą brane pod uwagę w analizach.
    c. Biała lista plików MIME - możliwość wykluczenia ze skanowania wskazanych plików typu MIME umieszczając je na białej liście, co pozwoli na uzyskanie mniejszej ilości wyników lepszej jakości i bardziej skuteczne zarządzanie bezpieczeństwem.
    d. Czarne listy typów plików – możliwe wykorzystanie, modyfikowalnej listy typów plików do wykrywania tylko określonych dokumentów, np. dokumentów pakietu MS Office, archiwów, plików wykonywalnych, plików graficznych, itp.
    e. Czarna lista plików – możliwość zidentyfikowania plików na podstawie ich nazwy i monitorowanie zmiany ich lokalizacji. W oparciu o te wyniki można sporządzić listy plików niedozwolonych i wykorzystać np. z funkcję usuwania, szyfrowania lub archiwizowania ich.
    f. Szyfrowanie danych - wybrane dane można zaszyfrować za pomocą silnego szyfrowania np. AES 256.
    g. Klasyfikację i oznaczanie plików - wybrane pliki można oznaczyć „niewidzialnym znacznikiem” (fingerprint),
    h. Monitoring i analiza - wynik działania procesów skanowania są dostępne w konsoli administracyjnej w postaci przejrzystych danych tabelarycznych oraz widżetów. Można zawęzić agregację danych za pomocą dowolnie definiowanych filtrów statycznych jak i dynamicznych,
    i. Eksport danych - każdą tabelę z danymi można wyeksportować do wielu formatów lub wysłać e-mailem do odpowiedniej osoby.
    j. Atrybuty plików skanowanych – można ograniczyć zakres skanowanych plików poprzez ustalenie przedziału rozmiaru pliku czy czasu utworzenia pliku.
    k. Usuwanie zbędnych danych – możliwość identyfikacji i usuwania/archiwizowania nadmiarowych lub zbędnych już dane (wymagania rozporządzenia RODO).
    l. Precyzyjne skanowanie wg szablonów – np. możliwość przeszukiwań za pomocą odpowiednich szablonów, takich jak ICD-9, ICD-10 - identyfikacja danych medycznych,
    m. Czarna lista treści – możliwość definiowania czarnych list treści takich jak numery PESEL, dowodów osobistych, kart kredytowych, kont bankowych i innych umożliwiających identyfikację osób celem znalezienia plików, miejsc ich

występowania i ilości duplikatów, pozwalających podejmować odpowiednie działania zabezpieczające,

n. Skanowanie plików i zawartości – możliwość tworzenia reguły identyfikacji treści chronionej w zależności od atrybutów pliku – nazwa, typ, szablonów treści, zawartość w celu wykonania skanowania zasobów sieciowych i lokalnych pod kątem występowania wybranych danych i późniejszych odpowiednich działań bezpieczeństwa na tych plikach.

16) Zapewniać ochronę danych w użyciu (bazującą na monitorowaniu prób dostępu do plików z wykorzystaniem certyfikowanych przez Microsoft sterowników) poprzez:

a. monitorowanie operacji na plikach – możliwość tworzenia reguł dostępu do plików (edycji, usuwania, modyfikacji, tworzenia); nadawanie użytkownikom odpowiednich praw do plików, niezależnie od ich lokalizacji oraz domeny
b. „biała lista" plików" MIME - możliwość wykluczania z monitorowania wybranych typów plików MIME, umieszczając je np. na białej liście (ograniczanie ilości zapisów z operacji na plikach w logach)
c. „biała lista plików" – możliwość definiowania listy plików w oparciu o szablon nazwy, rozszerzenie, rozmiar, datę utworzenia. Pliki taki są wyłączone z monitorowania, a działania użytkowników na tych plikach nie podlegają analizie.
d. monitorowanie drukowania - możliwość blokowania wydruku wybranym plikom i użytkownikom, możliwość budowania zaawansowanych reguł bezpieczeństwa wydruków.
e. „czarna lista plików" - możliwość monitorowania plików na podstawie ich atrybutów (nazwa, rozszerzenie, wielkość, data utworzenia) i monitorowanie dostępu do nich. Lista logów powinna pozwalać na analizę kto i kiedy uzyskał dostęp do pliku, zmodyfikował plik lub usunął plik.
f. „czarna lista typów plików" – możliwość wykorzystania modyfikowalnej czarnej listy typów plików do monitorowania tworzenia, edycji, usuwania, kopiowania zawartości. Możliwość ustawienia głównych typów chronionych plików, np. dokumenty pakietu MS Office, archiwa, pliki tekstowe, pliki graficzne itp.
g. monitorowanie plików oznaczonych – możliwość ustawiania specjalnych znaczników plików do identyfikacji plików podlegających odrębnym regułom monitorowania. Np. nie zezwalanie na dokonywanie zmian w tego typu plikach, monitorowanie ich kopiowanie i usuwania, monitorowania kopiowania treści z tych plików.
h. atrybuty plików monitorowanych - możliwość ograniczania zakresu monitorowanych plików poprzez ustalenie przedziału rozmiaru pliku czy zdefiniowanie okresu utworzenia pliku.
i. szyfrowanie danych – możliwość zaszyfrowania wybranych plików za pomocą silnego szyfrowania AES 256.
j. monitorowanie kopiowania zawartości – możliwość monitorowania i blokowania kopiowania zawartości dokumentów wybranym użytkownikom, możliwość budowania zaawansowanych reguł bezpieczeństwa kopiowania w oparciu o konkretną treść.
k. Monitorowanie „print screen" – możliwość monitorowania i blokowania użycia klawisza Print Screen, analizy kopiowanej treści pod względem występowania grafiki i tekstu.

l. Eksport danych - każdą tabelkę z monitorowanymi plikami można wyeksportować do wielu formatów lub wysłać e-mailem do danej osoby, możliwe do wykorzystania gotowych raporty w popularnych standardach
m. Monitoring i analiza – możliwość wykonywania zaawansowanych analiz działań użytkowników na poszczególnych plikach.

17) Zapewniać ochronę danych w ruchu, wykorzystując np.:
a. „czarne listy plików" – możliwość blokady transferu plików posiadających odpowiednie atrybuty (nazwa, rozszerzenie, wielkość, data utworzenia).
b. „czarne listy typów plików" – możliwość budowy czarnej listy plików bezwzględnie chronionych i zapobiegającej transferowi tych plików wybranymi kanałami.
c. Transfer plików zaszyfrowanych – możliwość zezwalania lub blokowania transferu plików szyfrowanych, np. wymuszanie zaszyfrowania plików przed transferem.
d. Transfer treści komunikatorami – możliwość monitorowania i blokowania transferu treści z wykorzystaniem komunikatorów.
e. Eksport danych - każdą tabelę z monitorowanymi plikami można wyeksportować do wielu formatów lub wysłać e-mailem do wybranej osoby.
f. Monitoring i analiza – możliwość wykonywania zaawansowanej analizy działań użytkowników na poszczególnych plikach.
g. Transfer plików ftp – możliwość monitorowania i blokowania transferu plików do/z serwera FTP
h. „biała lista plików" – możliwość zezwolenia na transfer plików z tzw. białej listy plików, tworzonej w oparciu o szablon nazwy, rozszerzenia, rozmiaru, czy daty utworzenia pliku
i. Biała lista plików MIME – udzielanie pozwolenia na transfer wybranych typów plików MIME, umieszczonych na białej liście.
j. Transfer plików e-mailem – możliwość monitorowania i blokowania transferu plików za pośrednictwem poczty elektronicznej
k. Monitorowanie kopiowania plików – możliwość tworzenia reguły monitorujących kopiowanie plików z dysku na dysk (np. lokalny), na dyski zewnętrzne
l. Monitorowanie treści – możliwość monitorowania treści w oparciu o analizę danych w spoczynku (okresowe skanowanie), bądź w oparciu o analizę danych w użyciu (np. edytowalny plik Word z treścią chronioną) i nadanie plikom niewidzialnych specjalnych znaczników. Tak oznaczone pliki podlegają specjalnej ochronie
m. Transfer plików do chmury – możliwość monitorowania i blokowania transferu plików do wielu popularnych chmur.

II. Budowa systemu, wymagania systemowe, interfejsy i funkcjonalności systemu

1. Budowa systemu

1.1. System musi posiadać łącznie 4 dostępy administracyjne umożliwiające działania administracyjne w konsoli systemu, jednego administratora w każdej wymienionej wyżej jednostce powiatu.

1.2. Architektura:

1.2.1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
1.2.1.1. Połączenie klient – serwer, komunikacja odbywa się z wykorzystaniem TLS ver. 1.3. Serwer i klient posiadają certyfikaty SSL 4096 bitowe.
1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, powinna być w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych).
1.2.3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach zgodnie ze specyfikacją opisaną poniżej.
1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.
1.2.5. Baza danych powinna umożliwiać pracę na silniku SQL w wersjach bezpłatnych (open source).

1.3. Konfiguracja Architektury:
1.3.1. Komponenty Klient, konsola administracyjna, serwer, baza danych muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu.
1.3.2. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja Klientów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie od producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją.
1.3.3. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, polityk, pomoc i inne wbudowane bazy wiedzy.
1.3.4. Klient do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI.
1.3.5. Klient musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku *.msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku *.msi.
1.3.6. System zapewnia możliwość stworzenia instalatora (.exe) z wbudowanymi, zaszyfrowanymi poświadczeniami dla dowolnego konta. Funkcja ta umożliwia instalację usługi bezpośrednio na kontach użytkowników – zarówno lokalnych, jak i

domenowych, korzystając z uprawnień zdefiniowanych dla instalatora w konsoli systemu.

1.3.7. Klient musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa).

1.3.8. System powinien umożliwiać generowanie unikatowego identyfikatora Klienta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków.

1.3.9. Klient musi mieć definiowalny priorytet pracy, przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów.

1.3.10. Klient musi wspierać wiele różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu Klienta.

1.3.11. System musi umożliwiać komunikację pomiędzy Klientami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.

1.3.12. System musi mieć możliwość współpracy komponentów Klient i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami Klientów.

1.4. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem.

1.4.1. Automaty powinny realizować co najmniej:

1.4.1.1. Usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nie przyrostowe, zmniejszanie bazy danych.

1.4.2. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie.

2. Wymagania systemowe

2.1. Konsola administracyjna musi działać w pełni responsywnie na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).

2.2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2016/2019/2022, Windows 7/8/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.

2.3. Serwer musi działać na systemach 64 bitowych Windows Server 2016/2019/2022.

2.4. Baza danych może działać na silniku w wersji 64 bitowych bezpłatnym ze wsparciem producenta (np. Microsoft SQL Server Express Edition).

2.5. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V.

3. Interfejsy

3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej z usługi MS Active Directory, przy

czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.

3.2. System musi umożliwiać import użytkowników z zewnętrznego pliku CSV.

3.3. System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switche itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane.

3.4. System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS.

3.5. System zapewnia integrację z modelem LLM.

4. Funkcjonalności systemu

4.1. Funkcjonalność Klienta

4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania Klienta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego).

4.1.2. Klient musi mieć możliwość konfiguracji zakresu skanowania plików.

4.1.3. Klient musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej, konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkowniku, który go wyświetlił.

4.2. Funkcjonalność konsoli administracyjnej.

4.2.1. Konsola musi być w pełni polskojęzyczna.

4.2.2. Interfejs konsoli musi zapewnić musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie).

4.2.3. Konsola administracyjna musi posiadać dashboard – dashboard użytkownika, dashboard prezentujący parametry infrastruktury, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie.

4.2.4. Konsola administracyjna musi być wyposażona w panel zawierający graficzne widżety prezentujące dane w postaci wykresów bądź w formie tabeli z danymi.

4.2.5. Dane na widżetach muszą być aktualizowane automatycznie.

4.2.6. System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widżety, ich konfigurację i kolejność).

4.2.7. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu.

4.2.8. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą mieć możliwość filtrowania kolumnowego.

4.2.9. System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w

opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.

4.2.10. Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko).

4.2.11. Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja Klienta, stanu Klienta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera.

4.2.12. Konsola musi zawierać w sobie pełną dokumentację systemu.

4.3. Odczytywanie zainstalowanego oprogramowania

4.3.1. System powinien prezentować podgląd zainstalowanych systemów operacyjnych, pakietów oraz aplikacji na komputerach z informacjami o: nazwie, wersji, producencie, typie licencji.

4.4. Wzorce aplikacji i pakietów

4.4.1. System ma posiadać wbudowaną obszerną bazę wzorców dostawcy oprogramowania.

4.4.2. System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania.

4.4.3. Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów.

4.4.4. System musi mieć możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera / komputerów wzorce mają być utworzone. Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu.

4.5. Inwentaryzacja sprzętu komputerowego

4.5.1. System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem).

4.5.2. System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language.

4.5.3. System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu).

4.5.4. System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania.

4.5.5. System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza począwszy od wskazanego miejsca w hierarchii kluczy rejestru.

4.5.6. System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu).

4.5.7. System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).

4.5.8. System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku.
4.5.9. System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu.
4.5.10. System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent).
4.5.11. System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne.
4.5.12. System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów.
4.5.13. System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik)
4.5.14. System umożliwia dodawanie notatek do każdej pozycji sprzętu.
4.5.15. System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).
4.5.15.1. System musi umożliwiać definiowanie typów serwisów
4.5.15.2. System musi umożliwiać definiowanie wartości serwisu
4.5.15.3. System musi umożliwiać definiowanie daty ważności serwisu oraz daty gwarancji
4.5.16. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium.
4.5.17. System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja).
4.6. Inwentaryzacja urządzeń podłączanych do komputera.
4.6.1. System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.)
4.6.2. System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika.
4.6.3. System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika).
4.7. Inwentaryzacja urządzeń sieciowych.
4.7.1. System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym IP/porcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać SNMP w wersji 1/2c/3.
4.7.2. Skaner SNMP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.
4.7.3. System musi zbierać informacje o jakości połączenia:
4.7.4. Czas odpowiedzi serwisów (usług) podawany w milisekundach:
4.7.4.1. Średni czas odpowiedzi.
4.7.4.2. Minimalny czas odpowiedzi.
4.7.4.3. Maksymalny czas odpowiedzi.
4.7.5. Ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat.

4.7.6. System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają Klienta.

4.7.6.1. Posiada niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci

4.7.6.2. Baza wzorców musi zawierać co najmniej 100 monitorowanych portów i usług.

4.7.6.3. System musi umożliwiać administratorowi definiowanie dodatkowych portów do monitorowania i przypisywanie do nich usług, a także modyfikowanie istniejących rekordów, obejmujących: port TCP, kategorię, nazwę usługi oraz nazwę skróconą.

4.7.7. System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci.

4.7.7.1. System musi umożliwiać generowanie map według dowolnych filtrów użytkownika.

4.8. Zdalna administracja komputerami

4.8.1. System ma automatyczne wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika.

4.8.1.1. System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu Windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania.

4.8.1.2. Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory Windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego.

4.8.1.3. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status).

4.8.1.4. System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, Windows PowerShell. System posiada co najmniej kilkadziesiąt predefiniowanych poleceń. System musi umożliwiać użytkownikom automatyczne definiowanie poleceń cmd/PowerShell. Funkcjonalność ta pozwala na wprowadzanie opisów zadanych czynności, a następnie, wykorzystując zaawansowane algorytmy AI, system automatycznie generuje adekwatne skrypty.

4.8.1.5. Zaawansowany Asystent AI do Przygotowywania Skryptów do precyzyjnego tworzenia szczegółowych skryptów

4.8.1.6. System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.).

4.8.1.7. System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)

4.8.1.8. System musi umożliwiać tworzenie zadań cyklicznych dla komputerów.

4.8.1.9. Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/drugi/trzeci/czwarty/ostatni poniedziałek/wtorek/środa/czwartek/piątek/sobota/niedziela/dzień wolny/dzień powszedni co n miesięcy, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania.

4.8.1.10. System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie.

4.8.2. System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro.

4.8.2.1. System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączanie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji.

4.8.2.2. System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6).

4.8.3. System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacja oprogramowania, poprawek i aktualizacji (service pack, patch).

4.8.3.1. System umożliwia zdalne podłączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii Ultra VNC.

4.8.3.2. System musi umożliwiać uruchomienie sesji Ultra VNC w trybie podłączenia się do obecnie zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejęcia dostępu).

4.8.4. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.

4.8.5. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.

4.9. Wysyłanie wiadomości

4.9.1. Komunikator

4.9.1.1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości pomiędzy użytkownikiem komputera z zainstalowanym Klientem a administratorem systemu.

4.9.1.2. Powinien zapewniać możliwość inicjowania czatu przez administratora.

4.9.1.3. Użytkownik powinien mieć opcję rozpoczęcia rozmowy za pomocą ikony na pasku zadań, która automatycznie uruchamia się zgodnie z konfiguracją Klienta.
4.9.1.4. System musi przechowywać historię konwersacji.
4.9.1.5. Powinien informować administratora poprzez powiadomienie w konsoli systemowej o nowych wiadomościach od użytkowników.
4.9.2. Wiadomość Jednorazowa:
4.9.2.1. System powinien umożliwiać wysyłanie jednorazowych wiadomości w trybie natychmiastowym jako ALERT.
4.9.2.2. Musi oferować możliwość wysłania wiadomości z opcją odłożenia na później (na 10 minut, 1, 2, 4 godziny) dla późniejszego odczytu.
4.9.2.3. Powinien zapewniać historię wysyłania i odbierania wiadomości przez użytkowników, z możliwością edycji treści w edytorze HTML.
4.9.2.4. Wiadomość powinna być dostępna do wysłania do określonej grupy, wybranych komputerów lub użytkowników.
4.9.2.5. System musi umożliwiać konfigurację czasu wygaśnięcia wiadomości.
4.9.3. Wiadomości Cykliczne:
4.9.3.1. Powinien pozwalać na tworzenie szablonów wiadomości do regularnego użytku.
4.9.3.2. Musi zapewniać funkcję odłożenia wysyłania wiadomości dla późniejszego odczytu, z możliwością edycji treści w edytorze HTML.
4.9.3.3. System powinien rejestrować historię wysyłania i odczytywania wiadomości przez użytkowników.
4.9.3.4. Powinien umożliwiać wysłanie wiadomości do zdefiniowanej grupy, wybranych komputerów lub użytkowników.
4.9.3.5. Musi oferować opcję konfiguracji terminu, po którym wiadomość wygaśnie.
4.9.4. System szkolenia pracowników za pomocą wiadomości.
4.9.4.1. System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów.
4.9.4.2. System musi posiadać predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa”, „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa”, „Postępowanie w przypadku naruszenia tajemnicy”, „Udostępnienie informacji stanowiących tajemnicę”.
4.9.4.3. Formatowanie treści musi być zgodne z HTML.
4.9.4.4. System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych).
4.9.4.5. System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców.
4.9.4.6. Użytkownik otrzymujący wiadomość musi być powiadamiany wizualne i dźwiękowo o otrzymaniu nowej wiadomości.
4.9.4.7. Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.
4.9.4.8. System musi udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników.
4.9.4.9. System musi generować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem).
4.10. Repozytorium – Centralna Baza Systemu

4.10.1.1. System musi posiadać wbudowaną centralną bazę systemu umożliwiająca import i eksport niektórych danych zarówno poprzez API jak też za pomocą wbudowanego import/eksporta.

4.11. Menedżer czasu pracy

4.11.1. System musi być wyposażony w zestaw statystycznych danych o pracy użytkownika i zdefiniowanych grup użytkowników.

4.11.2. System musi umożliwiać definiowanie dowolnej ilości grup użytkowników przypisanych do dowolnej ilości przełożonych.

4.11.3. System musi umożliwić wyświetlanie informacji o użytkowniku pobranych z Active Directory. Informacje powinny być aktualizowane zgodnie z harmonogramem połączenia z domeną.

4.12. Zarządzanie politykami bezpieczeństwa.

4.12.1. System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez bieżące (w czasie rzeczywistym) monitorowanie działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa oraz reguł ich opisujących.

4.12.2. System musi zapewniać automatyczne uruchamianie ochrony zasobów w czasie rzeczywistym zgodnie ze zdefiniowanymi politykami.

4.12.3. System musi zapewniać ciągłą ochronę danych niezależnie od położenia komputera (w sieci lokalnej, sieci VPN, poza siecią).

4.12.4. System musi na bieżąco monitorować i chronić za pomocą odpowiednio zdefiniowanych polityk i reguł dane w ruchu, dane w spoczynku oraz dane w użyciu.

4.12.5. Przez dane w spoczynku rozumie się dane, które nie są (ale mogą być) w ruchu lub w użyciu, wymagają inwentaryzacji i zabezpieczenia.

4.12.6. Przez dane w użyciu należy rozumieć dane, które są aktywnie przetwarzane przez dowolną aplikację i/lub punkt końcowy (komputer). Przykłady danych w użyciu: edycja dokumentu MS Word, Excel, PowerPoint, edycja pliku tekstowego CSV, TXT, tworzenie pliku, przechwytywanie ekranu (screenshot), kopiowanie / wklejanie danych.

4.12.7. Przez dane w ruchu należy rozumieć dane, które są przesyłane, np. kopiowanie danych (plików) z dysku sieciowego na nośnik USB, kopiowanie danych (plików) z komputera na komputer, przesyłanie danych e-mailem w treści lub w postaci załącznika, pobieranie danych z serwera FTP, przesyłanie danych za pomocą komunikatora.

4.12.8. Obiekty docelowe reguł muszą być definiowalne za pomocą parametrów takich jak: nazwa komputera, adres IP, unikatowy identyfikator agenta, status podłączenia do systemu (online/offline), zainstalowany system operacyjny, nazwę zalogowanego użytkownika, model komputera, producent komputera, dostawca komputera, budżet, z którego zakupiony został komputer, strukturę organizacyjną

4.12.9. Przy definiowaniu obiektów docelowych dla reguł DLP można korzystać ze znaków wieloznacznych.

4.12.10. System musi posiadać funkcjonalności monitorowania, blokowania, powiadomieniu użytkownika o wystąpieniu naruszenia zdefiniowanej polityki oraz pełnego logowania zdarzeń dotyczących polityki dla celów administracyjnych (powiadomienie administratora systemu).

4.12.11. System musi mieć możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP.

4.12.12. System musi mieć możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji.

4.12.13. Nowy komputer zgłaszający się do systemu po raz pierwszy musi bez dodatkowej ingerencji administratora automatycznie pobrać oraz wdrożyć (uruchomić) przeznaczoną dla niego politykę.
4.12.14. System musi mieć możliwość określenia ram czasowych działania danej reguły.
4.12.15. System musi dysponować mechanizmami dostępu do plików na poziomie jądra systemu operacyjnego MS Windows (32-bit i 64-bit), co uniemożliwia obejście zabezpieczeń nawet osobie z uprawnieniami administratora na poziomie systemu operacyjnego.

4.13. System musi w pełni wspierać następujące polityki ochrony danych:
4.13.1. Zdefiniowanie schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione.
4.13.2. Monitorowanie wykonywanych zrzutów ekranu, blokowanie możliwości zapisania i wykorzystania zrzutów ekranu.
4.13.3. Przechwytywanie zrzutów ekranu z komputerów użytkowników wyzwalany akcją użytkownika lub na życzenie administratora zgodnie z wcześniej ustawionym interwałem czasowym.
4.13.4. Umożliwienie powiadamianie o przekroczeniu dozwolonego czasu pracy komputera.
4.13.5. Wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku).

5. Kontrola i ochrona urządzeń
5.1. Blokowanie dostępu do wybranych typów urządzeń od strony sprzętowej. Wsparcie dla CD-ROM, portów USB, kart sieciowych, GPS, kart graficznych, modemów, klawiatur, czytników kart, drukarek, urządzeń Bluetooth i innych, monitorowanie podłączanych urządzeń.
5.2. Blokowanie dostępu do urządzeń USB, tworzenie czarnych list urządzeń, monitorowane podłączanych urządzań USB.
5.3. Zarządzanie dostępem do sieci społecznościowych, serwisów informacyjnych, blogów, bibliotek, forów dyskusyjnych oraz dowolnych stron www.
5.3.1. Blokowanie sieci ze względu na zdefiniowany typ i maskę sieci WIFI. Polityka musi zapewniać blokowanie dostępu do sieci zarówno otwartych jak i zabezpieczonych.
6. Klasyfikacja i ochrona dokumentów
6.1. Oznaczanie na dowolnym komputerze (znakowanie przez agenta) określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami.
6.2. Znakowanie określonych plików przechowywanych w zasobach serwerów lub udostępnionych zasobach (np. samodzielna macierz dyskowa) wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami, z wykorzystaniem harmonogramu.
6.3. Monitorowania i blokowania operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach.
7. Ochrona danych w użyciu
7.1. Podjęcie działania w momencie uruchomienia określonego procesu.
7.2. Podjęcie działań monitorowania i blokowania operacji w momencie próby kopiowania tekstu, zdjęcia czy ścieżki plików do schowka.

8. Ochrona danych w ruchu
   8.1. Monitorowanie danych przesyłanych za pomocą poczty e-mail oraz blokowanie przesyłania plików określonych typów.
   8.2. Monitorowanie danych przesyłanych do chmury oraz blokowanie synchronizacji plików określonych typów z wybraną chmurą.
9. Szyfrowanie dysków wewnętrznych
   9.1.1. System musi identyfikować partycje dysków twardych zaszyfrowane BitLockerem.
   9.1.2. System musi posiadać wbudowane mechanizmy do masowego zdalnego szyfrowania BitLockerem i wspierać metody XTS_AES_256, XTS_AES_128, AES_256, AES_128 oraz typy zabezpieczeń TPM+Pin, TPM, Passphrase.
   9.1.3. Ochrona danych na wbudowanych dyskach twardych musi być realizowana przez silne szyfrowanie całej zawartości dysku/dysków z wykorzystaniem MS API BitLocker oraz umożliwiać uwierzytelnianie użytkownika przed uruchomieniem startu systemu operacyjnego ze wsparciem metod silnego uwierzytelnienia.
   9.1.4. Ochrona danych przez szyfrowanie całej zawartości dysku oznacza, że szyfrowaniu podlegają wszystkie informacje zapisane na dysku twardym (łączenie z system operacyjnym, sterownikami, zainstalowanymi programami, danymi itp.).
   9.1.5. Funkcjonalność szyfrowania / deszyfrowania nie może być realizowana w oparciu o dodatkowego Klienta na stacji roboczej, lecz musi być integralnym rozwiązaniem oferowanego systemu.
   9.1.6. System musi umożliwiać zdalne szyfrowanie / deszyfrowanie partycji systemowych oraz niesystemowych oraz prezentować w konsoli administracyjnej bieżący postęp procesu.
   9.1.7. Szyfrowanie partycji niesystemowych polega na wprowadzeniu przez użytkownika hasła.
   9.1.8. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika komputera i może być realizowany w czasie jego pracy na komputerze. Szyfrowanie nie może być zostać wyłączone przez użytkownika.
   9.1.9. Proces szyfrowania może być zatrzymany podczas hibernacji oraz wyłączenia systemu, ale jest kontynuowany po wzbudzeniu / włączeniu komputera.
   9.1.10. System przechowuje klucze szyfrujące w konsoli administracyjnej, przy czym klucze są dostępne po dodatkowym uwierzytelnieniu administratora.
   9.1.11. System musi umożliwiać szyfrowanie / deszyfrowanie komputerów w sieci lokalnej oraz poza NATem.
   9.2. Szyfrowanie dysków zewnętrznych USB
   9.2.1. System musi identyfikować partycje dysków zewnętrznych zaszyfrowane BitLockerem.
   9.2.2. System musi posiadać wbudowane mechanizmy do masowego zdalnego szyfrowania / deszyfrowania BitLockerem i wspierać metody XTS_AES_256, XTS_AES_128, AES_256, AES_128 oraz typ zabezpieczeń Passphrase.
   9.2.3. Ochrona danych na zewnętrznych urządzeniach USB musi być realizowana przez silne szyfrowanie całej zawartości dysku z wykorzystaniem MS API BitLocker oraz umożliwiać uwierzytelnianie użytkownika przed dostępem do danych ze wsparciem metod silnego uwierzytelnienia.
   9.2.4. Funkcjonalność szyfrowania / deszyfrowania nie może być realizowana w oparciu o dodatkowego Klienta na stacji roboczej, lecz musi być integralnym rozwiązaniem oferowanego systemu.

9.2.5. Szyfrowanie partycji urządzeń USB polega na wprowadzeniu przez użytkownika hasła.
9.2.6. System musi umożliwiać zdalne szyfrowanie / deszyfrowanie partycji urządzeń USB oraz prezentować w konsoli administracyjnej bieżący postęp procesu.
9.2.7. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika komputera i może być realizowany w czasie jego pracy na komputerze. Szyfrowanie nie może być zostać wyłączone przez użytkownika.
9.2.8. System przechowuje klucze szyfrujące w konsoli administracyjnej, przy czym klucze są dostępne po dodatkowym uwierzytelnieniu administratora.

10. Monitorowanie uprawnień ACL
    10.1.1. System musi umożliwiać skanowanie list kontroli dostępu (ang., tzw. access-control list, ACL) z systemu katalogowego komputerów lokalnych oraz serwerów.
    10.1.2. Dane muszą zawierać: nazwę komputera, ścieżkę, właściciela folderu, nazwę grupy uprawnień, listę nadanych uprawnień, datę aktualizacji.
    10.1.3. Odczyt uprawnień na serwerach musi następować zgodnie ze zdefiniowanym harmonogramem.
    10.1.4. System musi posiadać predefiniowane filtry pozwalające na filtrowanie uprawnień do zasobów lokalnych oraz współdzielonych.
    10.1.5. Dane muszą być prezentowane w układach: Foldery -> Użytkownicy, Użytkownicy -> Foldery, Grupy -> Foldery, Właściciele -> Foldery.
11. Raportowanie i eksport danych
    11.1. System musi umożliwiać wyeksportowanie wybranych lub wszystkich danych do formatu .xls, .xlsx, .csv, .calc (OpenOffice), .html, .mht, .xml, .jpeg, .png, .gif, .bmp.
    11.2. System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów.
    11.3. System powinien umożliwiać eksport danych z raportu do formatów: pdf, xls, doc, rtf.
    11.4. System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).
    11.5. System musi istnieć możliwość tworzenia i dodawania własnych raportów przez użytkownika.
12. Bezpieczeństwo
    12.1. System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.
        12.1.1. Uwierzytelnianie do systemu musi być realizowane:
            12.1.1.1. z wykorzystaniem imiennego konta użytkownika i hasła,
            12.1.1.2. z wykorzystaniem imiennego konta administratorów aplikacji i hasła,
            12.1.1.3. za pośrednictwem uwierzytelniania poprzez Active Directory,
            12.1.1.4. za pośrednictwem uwierzytelniania poprzez CAS,
        12.1.2. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej.
        12.1.3. Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków).
        12.1.4. System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie (MFA).
            12.1.4.1. Uwierzytelnianie z wykorzystaniem obrazu wideo.

12.1.4.2. Uwierzytelnianie z jednorazowym kodem wysyłanym na e-mail użytkownika.
12.1.4.3. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe wraz z hasłem, które umożliwia jednoczesną pracę wielu użytkownikom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory/LDAP.
12.1.5. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania w oparciu o RSA 2048 bit, ECDSA 256 bit, DES/3DES, AES 256 bit, SHA-256.
12.1.5.1. Wykorzystywane klucze muszą posiadać wsparcie dla systemów Windows 7/8/10/11 i Windows Server 2016 i wyższe.
12.1.6. System musi umożliwiać blokadę dostępu po nieudanej próbie zalogowania się do systemu. Ponadto, system powinien oferować:
12.1.6.1. Podgląd wszystkich zablokowanych administratorów systemu, w tym informacje o typie, elemencie, czasie trwania blokady [s] oraz o ostatniej aktywności.
12.1.6.2. Możliwość odblokowania zablokowanego administratora systemu z poziomu konsoli administracyjnej przez osobę uprawnioną.
12.1.7. Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport.
12.1.8. System musi oferować możliwość podglądu wszystkich aktualnie otwartych sesji administratorów w konsoli administracyjnej, obejmując takie informacje jak: data utworzenia sesji, login, IP oraz SID.
12.1.8.1. Dodatkowo, system powinien umożliwiać wyszukiwanie zalogowanych administratorów po nazwie.
12.1.9. System musi udostępniać historię działań wybranych użytkowników/administratorów w zakresie, adresy URL i nagłówki http.
12.1.10. System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy Klientami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera.
12.1.11. System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nie przyrostowej oraz udostępniać informacje o rezultacie wykonania kopii.
12.1.12. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy).
12.1.13. System musi być wyposażony w mechanizmy powtórnego załadowania danych historycznych pochodzących od Klientów.
12.1.14. System musi zapewniać:
12.1.14.1. Pełne logowanie błędów w celu weryfikowania nieprawidłowości.
12.1.14.2. Przechowywanie logów systemowych.
12.1.14.3. Przechowywanie logów bezpieczeństwa.
12.1.14.4. Przechowywanie logów aktywności użytkowników i administratorów.
12.1.14.5. Pobieranie logów z Klientów z poziomu konsoli administracyjnej.
12.1.14.6. Możliwość eksportu logów.
12.1.14.7. Definiowanie maksymalnego czasu przechowywania plików log.
12.1.14.8. System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.

12.1.14.9. Definiowanie ścieżki do kopii zapasowej
12.1.14.10. Definiowanie ścieżki do importu danych
12.1.14.11. Definiowanie ścieżki do zapisu raportów
12.1.14.12. Definiowanie serwera do importu danych

13. Wsparcie i pomoc
    13.1.1. System musi posiadać dokumentację w postaci filmów instruktażowych/nagrań z webinariów w języku polskim.
    13.1.2. System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim.
    13.1.3. Pomoc techniczna
        13.1.3.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-15.00.
        13.1.3.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.
        13.1.3.3. Czas trwania usługi SLA wynosi od dnia zakupu do 11 marca 2026 r.
        13.1.3.4. Usługi Utrzymania Oprogramowania obejmują: asystę techniczną oraz świadczenie usług SLA, w ramach których realizowana jest obsługa zgłoszeń w zakresie: reakcja na zgłoszenia błędów, dokonywanie analizy przyczyn błędów, zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich, zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie infrastruktury zamawiającego, usuwania błędów w czasie naprawy, usuwania błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich – po udostępnieniu odpowiedniej aktualizacji przez producenta tego oprogramowania oraz jej uzyskaniu – w czasie naprawy;
        13.1.3.5. zapewnienie dostępności Oprogramowania.