Opis Przedmiotu Zamówienia

Zakup i wdrożenie oprogramowania zwiększającego poziom bezpieczeństwa Informatycznego.

Część 1. Oprogramowania EDR z konsolą do zarządzania w chmurze,

Część 2. Rozbudowa systemu backup-u, (158 licencji)

Część 3. Systemu do zarządzania infrastrukturą IT i zasobami ludzkimi

w ramach projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23 w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

1. Część 1. Oprogramowania EDR z konsolą do zarządzania w chmurze z wdrożeniem – 195 szt. licencji

1. Konsola zarządzająca

Charakterystyka

- Konsola web administratora powinna znajdować się w chmurze producenta znajdującej się na terenie Unii Europejskiej i zapewniać możliwość pełnego zarządzania stacjami roboczymi/serwerami przez przeglądarkę Web, która ma dostęp do Internetu.
- Konsola web administratora musi posiadać możliwość wyboru języka polskiego
- Konsola web musi umożliwiać zarządzanie stacjami roboczymi oraz serwerami i urządzeniami mobilnymi poprzez tą samą konsolę zarządzającą.
- Konsola web musi posiadać możliwość tworzenia grup i polityk dla stacji.
- Administrator musi mieć możliwość przenoszenia licencji pomiędzy urządzeniami stacjonarnymi i odrębnie między urządzeniami mobilnymi
- Administrator musi mieć możliwość zarządzania kluczem licencyjnym z poziomu konsoli administracyjnej.
- Konsola web musi umożliwiać bezpieczne logowanie do konsoli zarządzającej po protokole HTTPS z certyfikatem.
- Konsola web musi umożliwiać dwuetapową autoryzację logowania na minimum 2 sposoby.

- Konsola web musi posiadać możliwość zablokowania dostępu do ustawień programu ochrony dla użytkowników na urządzeniach nieposiadających uprawnień administracyjnych.
- Konsola web musi posiadać funkcję, która uniemożliwia użytkownikowi komputera wyłączenie działania monitora antywirusowego i innych składników ochrony, jeżeli nie posiada uprawnień administratora.
- Konsola web musi posiadać narzędzie do wykonania instalacji oprogramowania na stacjach poprzez Active Directory, grupy robocze lub zakresy adresów sieciowych IP.
- Konsola web musi umożliwiać wykonanie instalacji oprogramowania firm trzecich zdalnie z konsoli na stacjach bezpośrednio z bezpiecznego repozytorium dostawcy rozwiązania antywirusowego.
- Konsola web musi mieć możliwość zalogowania się kilku administratorom jednocześnie.
- Konsola web powinna oferować predefiniowane domyślne ustawienia rekomendowanych polityk (ustawień) dla stacji końcowych.
- Konsola web umożliwia zmianę ustawień priorytetu skanowania.
- Konsola web musi mieć funkcję planowania zadań, w tym planowania terminów automatycznego skanowania.
- Konsola web umożliwia wysyłanie powiadomień o zdarzeniach na wskazany adres mailowy.
- Konsola web musi posiadać możliwość uruchamiania komputerów zdalnie (WakeOnLAN), uruchamiania ponownego oraz wyłączania urządzeń z systemem Windows.
- Konsola web musi umożliwiać synchronizację z Azure Active Directory.
- Konsola web musi obsługiwać moduł do odbierania zgłoszeń serwisowych od użytkowników bezpośrednio z aplikacji zainstalowanej na stacji klienckiej.
- Rozwiązanie musi posiadać dedykowaną aplikację lub stronę internetową do zgłoszeń serwisowych bez konieczności instalacji ochrony antywirusowej.
- Konsola web musi posiadać zintegrowany moduł CRM z możliwością zaplanowania prac u użytkownika.
- Konsola web musi posiadać moduł uruchamiania procedur (skrypty) zdefiniowanych przez producenta oraz przez użytkownika w języku Python lub JSON.
- Oprogramowanie web musi zawierać zintegrowaną funkcjonalność menadżera aktualizacji (Patch Manager), który umożliwia zarządzanie pobieraniem aktualizacji (updatów) systemu Windows, Java, Adobe i innych producentów trzecich.
- Producent powinien posiadać własne bezpieczne i sprawdzone repozytorium aplikacji do celów aktualizacji oprogramowania firm trzecich minimum 50 producentów.

2. **Zarządzanie użytkownikami i stacjami**

- Rozwiązanie musi umożliwiać bezpośrednio z konsoli zarządzającej web uruchamianie procedur (skryptów) serwisowych na stacjach klienckich o minimalnych, następujących funkcjonalnościach:
    - Czyszczenie plików tymczasowych
    - Czyszczenie i sprawdzanie dysku
    - Usuwanie błędów dysku
    - Defragmentowanie dysku

  - Czyszczenie kolejki drukarki
  - Czyszczenie pamięci podręcznej DNS
  - Czyszczenie kosza
  - Sprawdzanie błędów na dysku twardym S.M.A.R.T. Check
  - Włączenie szyfrowania dysku funkcją Bitlocker dla systemu Windows
- System powinien przyjmować zgłoszenia serwisowe bezpośrednio z agenta na stacji, pocztą email oraz po przez dedykowaną stronę dla działu serwisu.
- System musi umożliwiać przydzielanie zgłoszenia serwisowego dla konkretnego administratora oraz powinien mieć zintegrowany system diagnozy stacji oraz możliwość podłączenia się poprzez zdalny pulpit.
- Konsola web musi posiadać zintegrowany moduł umożliwiający zdalne połączenie z graficznym pulpitem zdalnym przez dedykowaną aplikację dla komputerów/serwerów znajdujących się w sieci LAN i poza nią bez potrzeby tworzenia tuneli VPN każdej stacji komputera/serwera/Windows.
- Możliwość wyświetlania komunikatu przed połączeniem zdalnym pulpitem do użytkowania przez administratora w określonym przez niego czasie.
- Możliwość wyświetlania komunikatu przed połączeniem zdalnym pulpitem do użytkowania przez administratora w celu odpytania go o zgodę na połączenie.

3. **Agent ochrony konsoli – oprogramowanie antywirusowe**

- Konsola web musi mieć funkcję tworzenia raportów o stacjach w konsoli.
- Konsola web musi mieć funkcję logów wykonywanych czynności przez administratorów konsoli.

- Program antywirusowy powinien mieć obsługę w języku polskim. Platforma powinna obsługiwać systemy operacyjne:

  macOS:
  - 10.14.x
  - 10.15.x
  - 11.x
  - 12.x
  - 13.x
  - 14.x

  MS Windows (stacje klienckie):
  - Windows XP (SP3 or higher) x86
  - Windows 7 SP1 x86
  - Windows 7 SP1 x64
  - Windows 8 x86
  - Windows 8 x64
  - Windows 8.1 x86
  - Windows 8.1 x64
  - Windows 10 x86
  - Windows 10 x64
  - Windows 11 x64

MS Windows (wersja serwerowa):
- Windows Server 2003 SP2
- Windows Server 2003 R2 SP2
- Windows Server 2008 SP2
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

LinuxOS z gwarantowaną kompatybilnością:
- Latest Ubuntu 16.x LTS x64 release version (with GUI)
- Latest Ubuntu 18.x LTS x64 release version (with GUI)
- Latest Ubuntu 19.x x64 release version (with GUI)
- Latest Ubuntu 20.x LTS x64 release version (with GUI)
- Latest Ubuntu 21.04 x64 release version (with GUI)
- Latest Debian 8.x x64 release version (with GUI)
- Latest Debian 9.x x64 release version (with GUI)
- Latest Debian 10.x x64 release version (with GUI)
- Latest Red Hat Enterprise Linux Server 7.x x64 release version (with GUI)
- Latest Red Hat Enterprise Linux Server 8.x x64 release version (with GUI)
- Latest CentOS 7.x x64 release version (with GUI)
- Latest CentOS 8.x x64 release version (with GUI)

- Rozwiązanie powinno działać na komputerach wyposażonych minimalnie w:
  - 512 MB dostępnej pamięci RAM
  - 1 GB miejsca na dysku twardym dla wersji 32-bitowej i 64-bitowej
- Instalacja oprogramowania musi być możliwa poprzez Active Directory, grupy robocze, poprzez sieć, pobranie paczki MSI i za pomocą dystrybucji przez pocztę e-mail.
- Oprogramowanie powinno mieć możliwość przeglądania obciążenia procesów na stacji i serwerze oraz zawartości dysków z poziomu konsoli web.
- Ochrona poczty - antywirus musi chronić stacje poprzez uruchamianie nieznanych oraz niebezpiecznych załączników w środowisku wirtualnym na stacji takim jak lokalna i automatyczna piaskownica (auto-sandbox).
- Oprogramowanie umożliwia funkcję chat między administratorem konsoli a stacjami roboczymi (windows)
- Program antywirusowy musi posiadać możliwość skanowania wybranych plików, folderów/katalogów (również skompresowanych), a także całych dysków (w tym sieciowych) czy partycji.
- Oprogramowanie umożliwia cykliczne zrzuty ekranu podpiętych do konsoli stacji.
- Oprogramowanie umożliwia w konsoli WEB na:
  1. Podgląd uruchomionych procesów na danej stacji oraz ich zamknięcie
  2. Przeglądanie plików stacji końcowej
- 3. Podgląd uruchomionych usług oraz ich restart i zakończenie
  4. Wykonywanie poleceń CMD i Powershell w przeglądarce
  5. Podgląd systemowego dziennika zdarzeń
- Oprogramowanie umożliwia pełną wizualną personalizację aplikacji.

- Oprogramowanie umożliwia przypisanie aplikacji z repozytorium udostępnionego przez producenta
- Oprogramowanie umożliwia na rejestrowanie lokalne wszystkich zdarzeń z aplikacji oraz wysyłanie ich na zewnętrzny serwer SYSLOG
- Oprogramowanie umożliwia monitorowanie:

1. Monitorowanie wydajności pracy: CPU, RAM, sieci, dysku
2. Rozmiaru plików i folderów
3. Pojemności dysku
4. Aktywnych procesów
5. Podgląd dziennika zdarzeń systemu
6. Aktywnych połączeń sieciowych
7. Stron WWW
8. Zdarzeń aktualizacji systemu operacyjnego

- Program antywirusowy musi posiadać możliwość skanowania dowolnego zasobu podłączonego do stacji roboczej np.: dyski zewnętrzne, pamięci USB
- Program antywirusowy powinien posiadać filtering URL umożliwiający blokowanie konkretnych stron internetowych.
- Program antywirusowy musi posiadać moduł antywirusowy chroniący w czasie rzeczywistym.
- Program antywirusowy musi posiadać moduł sprawdzający reputację plików w chmurze.
- Program antywirusowy musi posiadać dwukierunkowy konfigurowalny z konsoli web firewall z możliwością tworzenia polityk globalnych i z podziałem na aplikacje.
- Program antywirusowy musi posiadać moduł HIPS (Host Intrusion Protection System – ochrona antywłamaniowa).
- Program antywirusowy musi posiadać moduł automatycznej piaskownicy (autosandbox), odizolowanego środowiska wirtualnego, w którym zasoby są emulowane dla obiektów w nim umieszczonych. Dodatkowo cały proces izolacji dzięki temu modułowi musi odbywać się lokalnie, na stacji roboczej. Całe środowisko wirtualne musi być odwzorowaniem 1:1 z systemem operacyjnym. Użytkownik powinien móc pracować w zwirtualizowanym środowisku, bez możliwości zapisu na stacji poza środowiskiem wirtualnym.
- Program antywirusowy musi posiadać możliwość uruchomienia dowolnego pliku/programu w automatycznej piaskownicy (auto-sandbox) na żądanie użytkownika (manualnie).
- Program antywirusowy musi umożliwiać użytkownikowi wysłanie podejrzanego obiektu do producenta oprogramowania antywirusowego w celu jego analizy. Funkcja ta powinna być dostępna z interfejsu programu antywirusowego.
- Podczas pracy komputera Program musi automatycznie skanować:
    - pliki uruchamiane, otwierane,
    - pliki kopiowane lub przenoszone,
    - pliki tworzone,
    - pliki pobierane z Internetu po protokole HTTP/HTTPS.
- W przypadku wykrycia wirusa program musi posiadać możliwość automatycznego poddawania kwarantannie podejrzanych obiektów oraz opcję przywrócenia z kwarantanny usuniętych obiektów.

- Program antywirusowy musi posiadać funkcję dodawania wyjątków do modułu antywirusowego, automatycznej piaskownicy (auto-sandbox) czy modułu HIPS.
- Program antywirusowy powinien posiadać dodatkowe narzędzie do skanowania systemu.
- Program antywirusowy musi posiadać dodatkowe narzędzie do analizowania bezpieczeństwa procesów.
- Program antywirusowy powinien mieć możliwość skanowania skompresowanych plików.
- Program antywirusowy musi być z możliwością zablokowania dostępu do zmiany ustawień programu hasłem administratora oraz hasłem skonfigurowanym w konsoli zarządzającej.
- Program antywirusowy powinien mieć możliwość importowania oraz eksportowania ustawień.
- Program antywirusowy powinien mieć możliwość tworzenia list zaufanych procesów.
- Program antywirusowy powinien mieć możliwość tworzenia list zaufanych plików.
- Program antywirusowy i konsola powinny umożliwiać tworzenie wyjątków ze skanowania folderów / plików.
- Program antywirusowy powinien umożliwiać konfigurację polityk (globalnych ustawień
  dla grup endpoint'ów) w celu szybkiej implementacji ustawień bezpieczeństwa dla wielu urządzeń.
- Program antywirusowy powinien umożliwiać zmianę ustawień priorytetu skanowania.
- Program antywirusowy powinien umożliwiać skanowanie pamięci komputera po uruchomieniu.
- Program antywirusowy posiada zintegrowaną funkcję skanowania i ochrony plików pod kątem danych wrażliwych (DLP).
- Program antywirusowy posiada zintegrowaną funkcję blokowania urządzeń zewnętrznych / przenośnych przed odczytem, edycją i zapisem plików w tym samym czasie.
- Program antywirusowy posiada zintegrowaną funkcję blokowania jedynie zapisu plików na urządzeniach zewnętrznych / przenośnych.
- Program antywirusowy powinien posiadać możliwość aktualizowania baz danych antywirusowych ręcznie, nawet jeśli komputer nie będzie miał dostępu do Internetu.
- Program antywirusowy musi posiadać zintegrowane środowisko, dzięki któremu możemy bezpiecznie działać w wirtualnym systemie nawet na zainfekowanej stacji. Środowisko to musi być odizolowanie od reszty systemu operacyjnego i mieć możliwość uruchomienia takich sesji bez wprowadzonych wcześniejszych zmian przez użytkownika w tym narzędziu (czyste środowisko). Ma również pozwalać na bezpieczniejsze wykonywanie przelewów bankowych, bez obaw, że system operacyjny, na którym działa dany komputer nie został uprzednio zmodyfikowany i byłby w stanie zagrozić utracie np. danych logowania do kont bankowych.
- Oprogramowanie powinno mieć możliwość przeglądania obciążenia procesów na stacji i serwerze oraz zawartości dysków z poziomu konsoli web.
- Oprogramowanie umożliwia funkcję chat między administratorem konsoli a stacjami roboczymi (windows)
- Oprogramowanie chroni przed nieupoważnionym zrzutem obrazu z ekranu.

- Oprogramowanie umożliwia analizę skryptu w programach pod kątem złośliwego oprogramowania przed ich uruchomieniem.
- Oprogramowanie umożliwia na rejestrowanie dzienników zdarzeń oraz zapisywanie ich lokalnie i na zewnętrznym serwerze.
- Oprogramowanie umożliwia personalizację wyglądu agenta ochrony.
- Oprogramowanie umożliwia zastosowanie proxy do rozpropagowania aktualizacji wewnątrz sieci.
- Oprogramowanie umożliwia procentową regulację zużycia zasobów procesora oraz nadania priorytetu.
- Oprogramowanie umożliwia śledzenie bibliotek uruchomionych przez procesy oraz blokowanie nieznanych bibliotek.

Dodatkowe systemy bezpieczeństwa

- Konsola web musi posiadać możliwość śledzenia historii zagrożeń na wybranych komputerach.
- Konsola web musi posiadać moduł zapobiegania wyciekowi danych DLP możliwością włączenia skanowania plików w wybranych lokalizacjach na komputerach pod kątem znajdujących się w nich danych wrażliwych przez zdefiniowane wzory z możliwością dodawania własnych reguł DLP oraz powinna umożliwiać sprawdzenia logów z tej czynności.
- Konsola web zintegrowana z wszystkimi poprzednimi modułami i funkcjami musi umożliwić przeprowadzenia skanowania sieci firmowej (również za pomocą protokołu SNMP) w celu przeprowadzenia audytu urządzeń działających w tej sieci.

4. **Moduł detekcji zagrożeń na urządzeniach końcowych**

- Rozwiązanie zawiera w sobie moduł oparty na technologii typu "Endpoint Detection & Response", zwany dalej EDR.
- Moduł EDR ma funkcję śledzenia zdarzeń systemowych i sieciowych urządzeń na których jest wdrożony.
- Moduł EDR ma funkcję alertowania wybranych zdarzeń, typowanych na stanowiące potencjalne zagrożenie dla cyberbezpieczeństwa, zgodnie z przyjętą polityką.
- Polityka bezpieczeństwa musi być edytowalna i mieć możliwość wprowadzania samodzielnie zdefiniowanych reguł. Nie jest dopuszczalne ograniczenie do reguł predefiniowanych przez producenta.
- Funkcja śledzenia zdarzeń musi mieć możliwość ich filtrowania względem co najmniej 10-ciu paramertów, w szczególności:
  a) urządzenia
  b) użytkownika
  c) podsystemu bezpieczeństwa
  d) techniki potencjalnego ataku.
  e) taktyki potencjalnego ataku.
- Moduł EDR musi mieć możliwość korelacji ewentualnych powiązań pomiędzy śledzonymi zdarzeniami i przedstawienia ich z użyciem sygnatur czasowych i/lub na osi czasu.

- Korelacja zdarzeń śledzonych przez EDR ma dotyczyć w szczególności:
  a) zmian w plikach
  b) zmian w rejestrze systemowym
  c) działających procesów i podprocesów
  d) dostępu do urządzeń zewnętrznych

5. **Dostawa, gwarancja i usługa wdrożeniowa**

- Dostawca zapewni wdrożenie rozwiązania u Zamawiającego w terminie nie późniejszym niż do 30 dni od podpisania umowy.
- Licencja na oprogramowanie ma mieć charakter subskrypcyjny
- Dostawa musi zawierać również:
  a. Wsparcie techniczne dystrybutora rozwiązań w języku polskim świadczone przez Inżyniera z certyfikatem Expert zatrudnionego przez autoryzowanego partnera składającego ofertę
  b. Szkolenie dla Administratorów z konfiguracji oferowanego rozwiązania przeprowadzone przez dystrybutora oferowanego rozwiązania w języku polskim
- Oferta musi być złożona przez autoryzowanego partnera
- Podmiot świadczący wsparcie techniczne musi posiadać Certyfikat ISO27001

Zamawiający dopuszcza rozwiązanie równoważne różnych producentów zgodne z opisem przedmiotu zamówienia pod warunkiem iż będą one posiadać jedną centralna konsole do zarządzania wszystkimi komponentami systemu oraz będą obsługiwane przez jedno centralne wsparcie techniczne w języku Polskim.

Część 2. Wymagania dla rozbudowy systemu backup-u z asystą przy wdrożeniu

Rozbudowa posiadanego systemu beckup-u Xopero One o dodatkowe licencje Endpoint Agent o 158 szt.

W ramach asysty przy wdrożenia wymagane jest zainstalowanie oprogramowania i konfiguracja na serwerze wirtualnym i szkolenie.

Część 3 . Systemu do zarządzania infrastrukturą IT i zasobami ludzkimi z wdrożeniem – 190 szt. licencji

W ramach wdrożenia wymagane jest zainstalowanie oprogramowania na serwerze wirtualnym wraz z konfiguracją i szkoleniem.

Specyfikacja systemu do zarządzania infrastrukturą IT i zasobami ludzkimi.

Zarządzanie zasobami
-Pozyskiwanie informacji o sprzęcie, zarządzanie widokami, funkcje ogólne
-Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania
-Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP oraz SNMP
-Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o aktualizacji
-Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy
-Odwzorowanie struktury organizacji w oparciu o Active Directory
-Jednostronna synchronizacja komputerów oraz drukarek z AD oraz AAD (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)
-Automatyczne skanowanie całości lub wybranych grup Active Directory (oraz AAD) oraz sieci
-Mapowanie atrybutów obiektów AD (oraz AAD) do obiektów w programie
-Grupowanie wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów, lokalizacji, statusów)
-Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.)
-Utworzenie własnych typów elementów wyposażenia
-Łączenie elementów wyposażenia w zestawy
-Przypisywanie zasobu do wielu zestawów
-Makrodefinicje w celu spersonalizowania nazw elementów w drzewku wyposażenia
-Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach
-Podpięcie dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików
-Przypisywanie sprzętu do konkretnych osób
-Przypisywanie sprzętu do wybranej firmy
-Automatyczne wyznaczanie 'Głównego użytkownika' komputera
-Wiązanie wielu rekordów wyposażenia z użytkownikiem
-Przypisywanie sprzętu do dowolnej lokalizacji
-Definiowanie własnych, dowolnych atrybutów sprzętu
-Aktywnym komputerom (bez określonego statusu) przydzielany jest status 'W użyciu'
-Wydruk etykiet z kodami kreskowymi do inwentaryzacji wyposażenia
-Dowolna treść kodu kreskowego
-Określanie loga firmy oraz użycia go na wydrukach
-Grupowa zmiana domeny/grupy roboczej zasobu

Informacje o sprzęcie
-Automatyczne wykrywanie typu komputera (Desktop\Notebook\Serwer\Kontroler domeny) na podstawie wyników skanowania sprzętu
-Wykrywanie komputerów typu All-In-One
-Automatyczne wykrywanie typów stacji roboczej (Tower\Desktop\SFF\uSFF)
-Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu
-Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM
-Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany
-Definiowanie statusów dla sprzętu (Nowy, Do kasacji, W serwisie, itd.)

-Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc.)
-Odczyt informacji o module TPM
-Odczyt D3Dscore z WinSAT
-Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: Switch, Router, Access Point, Bridge, Modem, NAS, UPS, itd.)
-Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu
-Automatyczne wykrywanie i tworzenie monitorów (producent, numer seryjny, rozdzielczość, odczyt firmy, działu, osoby odpowiedzialnej, głównego użytkownika)
-Automatyczne tworzenie zestawów: Komputer + Monitor
-Automatyczne utworzenie zestawów: Komputer + drukarka lokalna
-Automatyczne utworzenie zestawów: host + maszyny wirtualne
-Automatyczne wykrywanie czy komputer jest maszyną wirtualną
-Wykrywanie maszyn wirtualnych typu: Parallels Virtual Platform
-Określanie informacji o wykorzystywanej wirtualizacji
-Podgląd zestawów, do których należy zasób
-Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami
-Przypisywanie stałego atrybutu COA, który będzie uwzględniany na raportach wyposażenia i audytu
-Definiowanie szczegółowych informacji finansowych
-Obsługa walut w danych finansowych
-Definiowanie bazy dostawców sprzętu i oprogramowania
-Automatyczne odczytywanie ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu)
-Automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta
-Agent odczytuje identyfikator SID komputera
-Określanie adresu interfejsu webowego urządzenia sieciowego
-Określanie typu gwarancji dla zasobu
-Określenie wpływu biznesowego wybranego zasobu
-Tworzenie własnych typów gwarancji
-Określanie ikony dla typów zasobów
-Integracja z Dell API
-Wyszukiwanie i identyfikacja duplikatów zasobów
-Geolokalizacja komputerów z agentem

Raporty zasobów
-Raport dodanych załączników
-Automatyczne tworzenie historii zmian sprzętu
-Raport zbiorczy historii zmian w sprzęcie
-Ewidencja zdarzeń serwisowych
-Dodawanie notatek\komentarzy dla zdefiniowanych obiektów zasobów
-Informacja na temat pojemności dysków twardych oraz wolnego miejsca
-Wydruk\dodawanie jako załącznik protokołu przekazania\zwrotu\utylizacji sprzętu
-Wydruk\dodawanie jako załącznik protokołu przekazania dla całego zestawu
-Kreator szablonów wydruków WYSIWYG
-Definiowanie dedykowanych profili protokołów
-Zapisywanie protokołów podczas generowania jako załącznik do zasobu
-Wydruk\dodawanie jako załącznik Karty informacyjnej do elementu wyposażenia

-Wydruk lub zapis do pliku raportów ze szczegółami sprzętu
-Porównywarka wyników skanowania sprzętu
-Dzienniki zdarzeń systemu Windows
-Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu
-Geolokalizacja komputerów z agentem

Zarządzanie zasilaniem
-Zdalne włączanie i wyłączenie komputerów
-Obsługa SecureOn przy WakeOnLan
-Tworzenie harmonogramów wyłączania i włączania komputerów
-Wybór 5 trybów zamknięcia systemu: blokada komputera, uśpienie, hibernacja, wyłączenie, wymuszenie wyłączenia, restart
-Możliwość anulowania /wyświetlenia komunikatu jeśli jest zalogowany użytkownik
-Możliwość przerwania / odłożenia zadania na żądanie użytkownika
-Wymuszenie wylogowania użytkownika przed wyłączeniem komputera
-Raport zadań jednorazowych oraz harmonogramów
-Monitoring obciążenia CPU

Funkcje dodatkowe
-Zdalne wykonywanie skryptów (batch/powershell) - Obsługa zadań jednorazowych i cyklicznych
-Podpisywanie skryptów Powershell certyfikatem
-Wykonywanie skryptów w kontekście sesji użytkownika lub usługi
-Skrypty wykonywane po uruchomieniu komputera lub zalogowaniu użytkownika
-Wykonywanie zadań dla wszystkich komputerów
-Edytor skryptów z funkcją kolorowania składni
-Wykorzystywanie predefiniowanych skryptów
-Import informacji o wyposażeniu z pliku CSV
-Wyszukiwanie sterowników, informacji o komputerze, informacji o gwarancji w bazie producenta (DELL)
-Mechanizm automatycznego tworzenia rekordów producenta sprzętu (na podstawie wyników skanowania sprzętu)
-Generowanie kodów paskowych, QR dla każdego elementu wyposażenia
-Obsługa kodów QR

Archiwum zasobów
-Przeniesienie utylizowanego wyposażenia do archiwum
-Automatyczne usunięcie informacji sieciowych oraz licencji agenta dla zasobu archiwizowanego
-Zarządzanie sprzętem przez aplikacje mobilną
-Powiadomienia o kończącej się gwarancji\umowie serwisowej dla zasobu
-Zachowanie ostatniego skanu sprzętu podczas konserwacji bazy danych
-Powiadomienia o utworzeniu monitora, wykryciu maszyny wirtualnej-
-Grupowa zmiana atrybutów
-Personalizacja statusów zasobów

Zarządzanie oprogramowaniem
Licencje

-Inwentaryzacja licencji

-Automatyczne tworzenie licencji na podstawie kluczy produktów
-Odczytu OriginalProductKey (BIOS/UEFI) dla systemu operacyjnego
-Import licencji z pliku tekstowego
-Automatyczne generowanie historii zmian w licencji
-Określanie statusu licencji
-Tworzenie własnych atrybutów licencji
-Tworzenie notatek oraz załączników w dowolnym formacie do licencji
-Tworzenie licencji z poziomu rozliczenia audytu legalności
-Tworzenie licencji z poziomu raportu kluczy licencji
-Tworzenie zestawów licencji
-Relacja licencji z użytkownikiem, firmą, działem, lokalizacją
-Zmiana typu licencji dla wybranej grupy
-Kompletna informacja na temat posiadanych licencji (typ, producent, program licencjonowania, czas ważności, informacje finansowe)
-Przypisywanie licencji do komputera
-Definiowanie wymaganych atrybutów legalności (faktura, nośnik, COA, etc.)
-Definiowanie ilości posiadanych licencji w rozbiciu na użytkowników oraz stanowiska
-Definiowanie licencji przeznaczonych do przyszłego zakupu
-Definiowanie kluczy seryjnych i przypisywanie do licencji
-Automatyczne usunięcie wiązania pomiędzy zasobem archiwizowanym a licencją
-Określenie wpływu biznesowego wybranej licencji

Skanowanie oprogramowania
-Skanowanie oprogramowania na podstawie harmonogramu oraz definicji skanera
-Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecania skanów
-Śledzenie zmian w stanie zainstalowanego oprogramowania
-Zdalny skan komputerów (bieżący lub okresowy)
-Zmiana priorytetu skanowania oprogramowania
-Skan komputerów niepodłączonych do sieci
-Wysyłanie wyników skanowania offline na serwer FTP (Audyt)
-Przekazywanie konfiguracji wzorcowej dla skanera offline
-Identyfikacja zainstalowanych aplikacji na podstawie wzorców oprogramowania
-Prawidłowe rozpoznanie aplikacji nawet mimo zmiany jej nazwy
-Określanie masek plików dla publikacji elektronicznych (e-book)
-Skan plików skompresowanych
-Skan oraz identyfikacja zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lzh, lzma, msi, nrg, rar, tar, taz
-Wbudowane profile skanowania (np. profil wzorcowy)
-Definicja własnych ustawień skanowania
-Porównywanie wyników skanowania oprogramowania
-Wykrywanie plików multimedialnych
-Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika)
-Odczytywanie informacji o składnikach aplikacji, których programy instalacyjne nie są zgodne ze standardem MSI
-Identyfikacja SID użytkownika, dla którego zainstalowano oprogramowanie
-Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji\pakietów\systemów operacyjnych
-Nadpisanie bazy wzorców najnowszą, oficjalną bazą producenta

-Definiowanie katalogów wykluczonych / uwzględnionych w skanowaniu z wykorzystaniem symboli wieloznacznych (* , %)

Audyt oprogramowania
-Rozliczanie pakietów aplikacji
-Rozliczanie systemów operacyjnych
-Rozliczanie licencji typu „Downgrade”, "Upgrade" oraz instalacji innego oprogramowania w ramach licencji
-Audyt oprogramowania rozliczany automatycznie - informacja o stanie posiadanych licencji i faktycznie zainstalowanych programach z uwzględnieniem wybranych zestawów licencji.
-Historia audytów (Wyniki audytów powinny być przechowywane w bazie danych pozwalając na historyczny dostęp celem porównania i generowania raportów)
-Wsparcie procesu Audytu przez zaimportowanie materiału zdjęciowego i jego obróbkę
-Gotowe metryki audytowanego komputera - załącznik do protokołu przekazania stanowiska komputerowego (sprzęt + oprogramowanie)
-Uwzględnianie w rozliczeniu oprogramowania liczby aktywacji zapisanej w szablonie licencji

Funkcje
-Mechanizm informujący o nowej bazie wzorców oprogramowania
-Definiowanie własnych wzorców oprogramowania
-Automatyczne tworzenie wzorców oprogramowania dla systemów operacyjnych
-Automatyczne dodawanie informacji o wydawcy oprogramowania dla nowych wzorców, tworzonych na podstawie wyników skanowania
-Wykrywanie kluczy/identyfikatorów programów
-W przypadku aktywacji systemu Windows z użyciem serwera KMS, klucza MAK (Multiple Activation Keys) lub VLK (Volume License Keys) program powinien odczytywać przynajmniej 5 ostatnich znaków klucza
-Odczytywanie informacji o częściowych kluczach pakietów Microsoft Office
-Drukowanie lub zapisywanie do pliku raportów ze szczegółami oprogramowania
-Zbiorcze raporty wyników skanowania oprogramowania - Pakiety, pliki, systemy operacyjne, kluczy zainstalowanych aplikacji
-Raport z informacjami o pakietach oprogramowania uwzględniający parametry: przybliżona wielkość, adres strony internetowej, lokalizacja pliku instalacyjnego, architektura aplikacji, itd.
-Raport z informacjami o systemach operacyjnych uwzględniający parametry: Data instalacji, Architektura systemu, Wersja kompilacji, itd.
-"Wielkie raporty" (Możliwość utworzenia zbiorczych raportów obejmujących np. wszystkie przeskanowane pliki)
-Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (*.msi)
-Zdalna dezinstalacja oprogramowania
-Utworzenie harmonogramu dezinstalacji oprogramowania
-Generowanie skryptu deinstalacji aplikacji na podstawie otrzymanych wyników skanowania oprogramowania
-Raport stanu oprogramowania antywirusowego, anty-szpiegowskiego oraz zapory sieciowej
-Raport zainstalowanych aktualizacji systemu Windows

Kontrola wykorzystania sprzętu i oprogramowania
-Pozyskiwanie informacji o użytkownikach, zarządzanie widokami, funkcje ogólne

-Dane gromadzone dla konkretnych użytkowników (na bazie kont Windows) - jeden użytkownik może mieć przypisanych wiele kont Windows i pracować na różnych komputerach
-Odczyt informacji o kontach lokalnych komputera, wraz z odczytem grup do, których konto należy
-Grupowanie użytkowników z podziałem na jednostki organizacyjne w firmie (np. względem działów)
-Określanie firmy do której należy użytkownik
-Określanie przełożonego dla użytkownika
-Prezentacja 'stanu użytkownika' (obecny, nieobecny, nowy).
-Prezentacja 'statusu użytkownika' (Zatrudniony, zwolniony, itd.)
-Zarządzanie stanowiskami użytkowników
-Przeniesienie rekordu użytkownika do archiwum
-Funkcjonalności automatycznego generowania zmian rekordu użytkownika – Historia użytkownika
-Odczytywanie informacji o użytkownikach z Active Directory oraz AAD
-Pełna synchronizacja rekordów użytkowników (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory oraz AAD)
-Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień
-Podgląd zdjęcia przypisanego do użytkownika
-Przypisywanie do użytkownika załączników (pliki)
-Przypisywanie notatek do użytkownika
-Ewidencja zdarzeń przypisanych do użytkowników
-Automatyczne tworzenie działów na podstawie informacji odczytanych z Active Directory

Raporty
-Analiza aktywności użytkowników
-Grupowanie danych według komputerów jeśli użytkownik wykorzystywał więcej niż jedno stanowisko
-Analiza zdarzeń sesji użytkownika (logowanie, wylogowanie, zablokowanie, odblokowanie, nawiązanie połączenia RDP, zakończenie połączenia RDP)
-Analiza przerw w pracy
-Analiza jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków)
-Analiza aktywności mikrofonu oraz kamery
-Analiza wykorzystania poszczególnych aplikacji w czasie
-Analiza czasu działania aplikacji, na pierwszym planie oraz sumarycznie
-Uwzględnienie lub wyłączenie z raportu aplikacji bez aktywności użytkownika
-Kategoryzacja danych czasu pracy (czas pozytywny, neutralny oraz negatywny).
-Statystyki najczęściej wykorzystywanych aplikacji
-Statystyki wykorzystania komputerów przez poszczególnych użytkowników
-Statystyki aktywności użytkownika i grup użytkowników
-Generowanie raportów z monitoringu użytkowników dla wybranego zakresu godzin
-Kontrola wydruków - historia zadań drukowania zainicjowanych przez poszczególnych użytkowników
-Kontrola wydruków - Monitoring wydruków obejmuje szczegółowe parametry (np. format papieru, orientacje, skalowanie, itd.)
-Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz-b/kolor, dpi)
-Monitoring wydruków na drukarkach sieciowych
-Monitoring użytkowników stacji terminalowych

-Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.)
-Informacje o awariach, poczynaniach użytkowników: zakończonej aktualizacji, akcji podpięcia przenośnych dysków, włożenia płyt do napędów CD/DVD, śledzenie uruchomienia aplikacji przez użytkownika, monitoring informujący o małej ilości miejsca
-Raport zbiorczy historii zmian w rekordach użytkowników

Funkcje
-Blokada niepożądanych aplikacji. Programy mogą być blokowane dla całej firmy lub tylko dla wybranych użytkowników.
-Autoryzacja nośników zewnętrznych na podstawie wykrytych urządzeń
-Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych
-Automatycznie budowana baza informacji o napędach zewnętrznych
-Blokada dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.)
-Odczyt i blokada urządzeń PTP/MTP
-Określanie praw dostępu w zależności od typu urządzenia, np. Pendrive, CD/ROM
-Komunikacja z użytkownikami (Skype, mail) bezpośrednio z zakładki Użytkownicy
-Informacje o ostatnio zalogowanych osobach na stacjach klienckich
-Automatyczne tworzenie licencji – Dodawanie do licencji użytkowników, którzy są głównymi użytkownikami komputera, na którym wykryto licencje
-Komentowanie przerw pracy
-Kategoryzacja przerwy w pracy na podstawie komentarza

Kontrola wykorzystania Internetu
Funkcje
-Blokada stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokada WWW po zawartości (ContentType)
-Blokada stron internetowych dla protokołu http \ https w najpopularniejszych przeglądarkach WWW
-Kategoryzacja stron internetowych
-Import stron WWW z pliku lub ze schowka
-Slowniki kategorii stron WWW
-Blokada dostępu do witryn zgodnie z harmonogramem
-Blokada trybu incognito w przeglądarce Google Chrome

Raporty
-Raporty dotyczące aktywności użytkowników w Internecie
-Analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki)
-Monitoring stron internetowych dla protokołu http \ https (Edge, Chrome, Opera, Vivaldi, Firefox)
-Analiza liczby wejść na poszczególne strony lub domeny
-Kategoryzacja odwiedzanych domen i stron
-Raport informujący o plikach pobranych przez przeglądarki WWW
-Raport informujący o danych wysłanych przez przeglądarki (bez Firefox)
-Monitoring plików pobieranych przez przeglądarki internetowe

Helpdesk
Obsługa
-Rejestracja i obsługa zgłoszeń

-Obsługa zgłoszeń w modelu Kanban
-Określanie relacji pomiędzy zgłoszeniami (np.. Kopia, Incydent nadrzędny)
-Edycja zgłoszeń powiązanych w oknie zgłoszenia bieżącego
-Kategoria zgłoszeń może posiadać swojego opiekuna, który może zarządzać każdym zgłoszeniem danej kategorii
-Komentarze zgłoszenia obsługujące HTML oraz osadzanie obrazów
-Opis zgłoszenia w formacie HTML
-Nawiązywanie połączeń zdalnych bezpośrednio z edytora incydent
-Tworzenie notatek dla zgłoszeń
-Zapisywanie wersji roboczej komentarza
-Archiwizacja zgłoszeń
-Monitoring czasu pracy nad incydentem (time tracking)
-Raport ewidencji czasu pracy nad zgłoszeniem
-Informacja o czasie reakcji do podjęcia zgłoszenia
-Dodanie prywatnego komentarza
-Znaki @ oraz # pozwalają na wspominanie użytkownika oraz wpisu bazy wiedzy w komentarzu zgłoszenia
-Dodanie załączników do incydentów, również do komentarza
-Określanie dodatkowych subskrybentów dla notyfikacji e-mail dotyczącej zmian w incydencie
-Określanie uprawnień do incydentów (Publiczne, Prywatne, dla określonych działów)
-Zarządzanie filtrami zdefiniowanymi dla listy zgłoszeń
-Obsługa nazwy DNS oraz adresów IP (IPv4, IPv6) dla zgłoszeń
-Wydruk historii zgłoszenia
-Widok kalendarza (Planowanie rozwiązania incydentów)
-Korelacja incydentu z elementem zasobów
-Raport zbiorczy historii zmian
-Tworzenie i planowanie zastępstw, osoba zastępująca otrzymuje na czas zastępstwa dostęp do obsługi zgłoszeń osoby zastępowanej
-Wyszukiwanie komentarzy przy użyciu funkcji globalnego wyszukiwania
-Czas reakcji oraz realizacji wyznaczany automatycznie na podstawie umów SLA
-Automatyczne podpowiedzi rozwiązań dostępnych w bazie wiedzy na podstawie wpisywanego tematu
-Określenie wpływu biznesowego wybranego zgłoszenia
-Podgląd wiadomości źródłowej przy tworzeniu zgłoszenia lub komentarza na podstawie zgłoszeń email
-Duplikacja i replikacja zgłoszeń
-Powiadomienia o liczbie nieprzeczytanych zgłoszeń
-Automatyzacja obsługi zgłoszeń z wykorzystaniem utworzonych reguł

Konfiguracja
-Architektura drzewa dla kategorii zgłoszeń
-Tworzenie szablonów odpowiedzi
-Cykliczne raportowanie Listy incydentów
-Tworzenie własnych dodatkowych atrybutów dla zgłoszeń
-Personalizowane szablony wiadomości email z możliwością ustawienia stałego załącznika
-Notyfikacje e-mail o utworzeniu\zmianie\usunięciu incydentu
-Notyfikacje e-mail o zbliżających się terminach realizacji incydentu (Deadline)
-Automatyczny import wiadomości e-mail, jako zgłoszeń helpdesk (POP3 oraz IMAP)

-Import zgłoszeń helpdesk ze skrzynek współdzielonych (shared mailbox)
-Obsługa wielu kont pocztowych (Import + notyfikację email)
-Tworzenie własnych trybów oraz priorytetów incydentów
-Personalizacja widoku raportu listy incydentów
-Profile zgłaszających w helpdesk
-Personalizacja kolorów statusów zgłoszeń
-Automatyczne przypisywanie zgłoszeń do użytkowników
-Weryfikacja wiadomości źródłowych pobieranych z serwera pocztowego
-Konfiguracja maksymalnej wielkości załącznika

Moduł połączeń zdalnych
-Operacje na plikach i katalogach
-Zarządzanie procesami i rejestrem
-Monitoring pracy wykonywanej na komputerze
-Zdalny podgląd pulpitów wielu stacji w miniaturach ekranów
-Wywoływanie Windows Remote Desktop na danej stacji z poziomu aplikacji
-Wysyłanie wiadomości do użytkowników
-Uruchamianie na stacjach programów z wiersza poleceń Command Line
-Zdalne uruchamianie komputera za pomocą funkcji Wake-On-Lan
-Wake-On-Lan pozwala na definicję portu oraz adresu komputera docelowego
-Przejęcie kontroli nad stacją roboczą
-Blokada klawiatury i myszki na stacji klienckiej w trakcie przejęcia kontroli pulpitu zdalnego
-Przesyłanie kombinacji klawiszy Ctrl + Alt + Delete w zdalnym pulpicie
-Przejęcie kontroli nad komputerem bez zalogowanego użytkownika
-Wysyłanie pytania o zgodę na zdalny dostęp lub wysyłania komunikatu z informacją o rozpoczęciu podglądu pulpitu
-Podgląd pulpitu zdalnego w osobnym oknie z opcją fullscreen
-Obsługa wielu monitorów dla podglądu pulpitu
-Wybór monitora, z którego ma być przekazywany obraz podglądu pulpitu
-Nawiązywanie połączenia pulpitu zdalnego z wieloma komputerami jednocześnie
-Połączenie pulpitem zdalnym w konfiguracji NAT-NAT
-Zarządzanie usługami systemu Windows
-Raport Sesje zdalnego pulpitu
-Wybór adresu IP, na którym ma być zestawione połączenie zdalne
-Wybór portu, na którym klient nasłuchuje połączenia zdalnego
-Wykorzystanie protokołu autorskiego lub MS RDP do połączeń zdalnych

Baza wiedzy
-Wbudowana baza wiedzy
-Artykuły bazy wiedzy mogą być przypisane do kategorii zgłoszeń helpdesk
-Kopiowanie artykułów
-Edytor HTML
-Osadzanie załączników w treści artykułów
-Osadzanie multimediów w treści artykułów
-Baza wiedzy pozwala na tworzenia artykułów prywatnych oraz publicznych
-Szybkie kopiowanie wpisów bazy wiedzy
-Artykuły bazy wiedzy mogą zostać powiązane ze zgłoszeniami z systemu helpdesk

-Artykuły bazy wiedzy mogą zostać przypięte, dzięki czemu zawsze będą widoczne na liście artykułów
-Informacja o liczbie odsłon artykułu bazy wiedzy
-Bezpośrednie linkowanie artykułów bazy wiedzy

SLA
-Definiowanie planów umów SLA
-Definiowanie czasu obowiązywania umów SLA
-Definiowanie czasu pracy działów wsparcia technicznego
-Definiowanie dni wolnych na podstawie kalendarza świąt i dni wolnych
-Definiowanie czasów reakcji oraz realizacji zgłoszenia
-Notyfikacje mailowe o zbliżających się terminach reakcji oraz realizacji
-Automatyczne przypisanie umowy SLA do zgłoszenia na podstawie informacji o rozwiązującym, temacie wiadomości, priorytecie, kategorii, opisie
-Raportowanie o statusie i postępie w realizacji zgłoszeń z przypisaną umową SLA

Centralne repozytorium załączników
Funkcje
-Załączniki przechowywane w centralnym repozytorium
-Utworzenie relacji załącznika z innymi elementami systemu 1 - N (jeden do wielu)
-Dodawanie i modyfikacja załączników z poziomu innych zasobów
-Załączniki typu: link, udział oraz plik
-Pełna informacja o załączniku: twórca, data utworzenia, rozmiar, nazwa pliku, miniatura
-Historia zmian załącznika

Zarządzanie użytkownikami
Funkcje
-Raportowanie aktywności pracy
-Przeglądanie ostatnio zgłoszonych incydentów
-Powiązanie użytkownika z licencją
-Dostęp webowy do statystyk monitoringu, zgłoszeń helpdesk oraz powiązanych z użytkownikiem zasobów
-Cykliczne, automatyczne generowanie raportów
-Generowanie raportu obecności / nieobecności użytkownika wraz z korelacją jego aktywności na komputerze
-Zgłoszenia dotyczące wniosków nieobecności użytkowników
-Automatyczne typowanie użytkowników zastępujących dla zgłaszanych nieobecności
-Zarządzanie wnioskami nieobecności użytkowników przez przełożonych, informowanie przełożonych N poziomów wyżej o urlopie użytkownika
-Automatyczne utworzenie relacji przełożony - podwładny na podstawie skanów Active Directory
-Możliwość drukowania karty informacyjnej użytkownika, zawierającej informacje kontaktowe, informacje o powiązanych zasobach, licencjach oraz dostępy nadane w module RODO
-Generator struktury organizacji na podstawie powiązań użytkowników i ich przełożonych
-Planowanie dni wolnych w widoku kalendarza
-Planowanie zastępstw podczas nieobecności

Raportowanie cykliczne
Użytkownicy

-Raport historia sesji
-Raport Nośniki danych
-Raport Operacje na plikach
-Raport wydruków
-Raport użycia aplikacji
-Raport nagłówów okien
-Raport odwiedzonych stron WWW
-Najczęściej odwiedzane strony internetowe
-Raport Wysyłane pliki
-Raport czasu pracy przy komputerze
-Raport zestawienia kategoryzacji czasu pracy przy komputerze

Zasoby
-Raport historii zasobów
-Raport informujący o nowych zasobach
-Raport informujący o nadchodzących terminach w zasobach
-Raport Zasoby zarchiwizowane
-Raport Systemy Operacyjne

Podstawowe
-Raport Informacje o autoryzowanych agentach

Oprogramowanie
-Raport zainstalowanego oprogramowania
-Raport Szczegóły plików

Helpdesk
-Raport incydentów (Helpdesk)
-Raport czasu pracy nad zgłoszeniem
-Raport Czasy SLA

Automatyzacja
Lista dostępnych reguł

Ogólne
-Wygaśnięcie certyfikatu SSL
-Kończące się licencje na agenta
-Zapełniona baza danych
-Zbyt duży rozmiar folderu cache

Zasoby
-Brak połączenia od agenta
-Brak wolnej przestrzeni na dysku
-Ostrzeżenie od Windows Security Center
-Zakończenie skanowania sprzętu
-Dodanie zasobu
-Zmiana zasobu
-Usunięcie zasobu

-Zakończenie okresu gwarancyjnego
-Zakończenie umowy serwisowej
-Powielenie zasobów

Oprogramowanie
-Zmiana oprogramowania
-Zakończenie skanowania oprogramowania
-Zamknięcie audytu

Licencje
-Dodanie licencji
-Zmiana licencji
-Usunięcie licencji
-Wygaśnięcie licencji
-Planowana wymiana licencji

Użytkownicy
-Dodanie użytkownika
-Zmiana użytkownika
-Usunięcie użytkownika
-Logowanie użytkownika
-Wylogowanie użytkownika

Helpdesk
-Dodanie zgłoszenia
-Usunięcie zgłoszenia
-Zmiana zgłoszenia
-Brak aktywności w zgłoszeniu

Lista dostępnych Akcji
-Wykonywanie skryptu na podstawie zdefiniowanej reguły
-Wysłanie powiadomienia w konsoli zarządzającej na podstawie zdefiniowanej reguły
-Wysyłanie powiadomienia mailowego na podstawie zdefiniowanej reguły (inicjator zdarzenia, Administratorzy, konkretny użytkownik, rozwiązujący, zgłaszający, subskrybenci)
-Modyfikacja zasoby / użytkownika / zgłoszenia - w zależności od reguły
-Dodanie komentarza (dla reguł Helpdesk)
-Wysyłka wiadomości SMS

RODO
Funkcje

-Inwentaryzacja zbiorów danych, dostępów oraz powierzeń do zbiorów danych, dokumentów bezpieczeństwa, historii naruszeń bezpieczeństwa, szkoleń oraz wniosków o zapomnienie
-Wydruk raportów tabelarycznych: czynności przetwarzania, dostępów, powierzeń, listy dokumentów, statystyki zgłoszeń RODO, listę szkoleń, historii naruszeń bezpieczeństwa, wniosków o zapomnienie
-Wydruk wniosków o nadanie uprawnień, modyfikacji oraz anulowania upoważnienia
-Wstępne wypełnienie wniosków o zmianę dostępu

-Utworzenie zgłoszeń za pomocą przycisków szybkiej akcji
-Delegowanie zadań w helpdesk dla osób odpowiedzialnych za zbiory danych
-Archiwizacja zbiorów
-Definiowanie czynności przetwarzania
-Przypisywanie zbioru danych do czynności przetwarzania
-Przydzielanie dostępów do czynności przetwarzania
-Zapisywanie historii zmian wniosków o dostęp do zbiorów
-Dodawanie historycznych dostępów oraz wniosków o dostęp
-Filtrowanie użytkowników w raporcie Dostępy

Raporty
-Raport zbiorczy Czynności przetwarzania
-Raport zbiorczy Zbiory danych
-Raport zbiorczy zinwentaryzowanych dostępów
-Raport zbiorczy zinwentaryzowanych powierzeń
-Raport zbiorczy zinwentaryzowanych dokumentów
-Raport zbiorczy historii naruszeń bezpieczeństwa
-Raport zbiorczy wniosków o dostęp
-Raport zbiorczy Dostępy

Sygnalista
Funkcje
-Tworzenie zgłoszeń w postaci anonimowej lub nieanonimowej
-Usuwanie metadanych z załączników zgłoszeń
-Usuwanie danych osobowych ze zgłoszeń
-Podział interfejsu na publiczny oraz dla wewnętrzny
-Dashboard podsumowujący wykorzystanie portalu sygnalisty
-Przypisywanie rozwiązujących zgłoszenia sygnalistów w zależności od typu zgłoszenia lub jego źródła
-Definiowanie własnych atrybutów, kategorii, trybów zgłoszeń oraz poziomów ryzyka
-Definiowanie stron publicznych (dostępnych dla sygnalistów)
-Obsługa wielu języków stron publicznych
-Natywne wsparcie języka ukraińskiego
-Definiowany limit załączników
-Wyróżnienie zgłoszeń o przekroczonym czasie reakcji

Raporty
-Raport zgłoszeń
-Historia zmian
-Statystyka zgłoszeń
-Pozostały czas na przyjęcie zgłoszenia
-Pozostały czas do zakończenia
-Widgety: Kategorie zgłoszeń, Poziomy ryzyka, Tryby zgłoszeń, Statusy zgłoszeń, Ostatnio dodane

Portal Web
Funkcje

-Wallboard - ekran zbiorczy prezentujący wybrane informacje z całego systemu

-Dashboard każdego modułu z najważniejszymi informacjami w postaci widgetów
-Widok zawierający oś czasu z aktywnością użytkownika
-Rozbudowane filtry dla raportów tabelarycznych
-Zarządzanie użytkownikami, agentami, zasobami, licencjami, działami, audytami
-Konfiguracja portalu helpdesk, kont administracyjnych oraz organizacji
-Raporty dla każdego modułu w formie tabelarycznej
-Obsługa helpdesk oraz bazy wiedzy
-Obsługa modułu RODO
-Obsługa modułu automatyzacja
-Obsługa kanału zgłoszeń wewnętrznych dla Sygnalistów
-Automatyczne logowanie przy pomocy aplikacji
-Logowanie za pomocą poświadczeń domenowych (SSO)
-Logowanie za pomocą konta AzureAD lub AAD
-Wydruk raportów tabelarycznych
-Kontrola statystyk użytkowników
-Menu szybkiego dodawania nowych elementów (użytkownik, nieobecność, zasób, licencja, zgłoszenie, artykuł bazy wiedzy, zbiór danych, czynność przetwarzania)
-Przełączanie wersji językowej bez ponownego logowania do systemu
-Nawigacja Breadcrumb

Funkcjonalności ogólne
-Określanie praw dostępu do grup zasobów lub użytkowników
-Aplikacja desktopowa służąca do zarządzania systemem może być zainstalowana na dowolnej liczbie komputerów ("Licencja pływająca")
-Dodatkowa aplikacja webowa umożliwiająca dostęp do systemu i zarządzanie systemem
-Wersja angielska (en-US) interfejsu użytkownika
-Praca w oparciu o silniki baz danych: MS SQL lub PostgreSQL
-Swobodna migracja danych pomiędzy MS SQL i PostgreSQL
-Zdalna instalacja i dezinstalacja agentów na stacjach roboczych
-Odczytywanie struktury organizacji z Active Directory
-Skaner sieci wykorzystywany do wykrywania nowych urządzeń
-Mechanizm automatycznego tworzenia komputera na podstawie danych przesłanych przez agenta
-Mechanizm automatycznego tworzenia użytkowników na podstawie danych przesłanych przez agenta
-Automatycznie dodane komputery\użytkowników są powiązane z odpowiednią grupą zgodną z OU w Active Directory
-Definiowanie nieograniczonej liczby użytkowników systemu
-Określanie ról dla kont systemu na przykład Administratorzy, Menadżerowie, Zarządcy, Pracownicy
-Indywidualny login i hasło dla poszczególnych użytkowników
-Automatyczne logowanie do systemu
-Zarządzanie uprawnieniami użytkowników - określanie dostępu do poszczególnych obiektów systemu (konkretny użytkownik, konkretny zasób lub ich grupy) , możliwość ograniczenia operacji (wyświetlanie, tworzenie, edycja, usuwanie)
-Dostęp do programu chroniony przy pomocy uwierzytelniania wieloskładnikowego
-Określanie ról użytkowników - zarządzanie grupami
-Zabezpieczenie Agentów przed nieautoryzowanym wyłączeniem lub usunięciem
-Eksport danych do plików zewnętrznych (Excel, html, CSV, PDF, TXT, MHT, RTF, BMP)

-Zgodny z pracą w sieciach WLAN
-Podgląd aktualnych zadań serwera
-Centrum informacji - przekrojowy raport na temat zdarzeń oraz statusu monitorowanych komputerów i użytkowników
-Wielopoziomowe drzewo lokalizacji oraz relacje lokalizacji z firmami
-Wyszukiwanie danych w tabelach raportów
-Dowolne definiowania grup sprzętu i użytkowników
-Tworzenie dowolnych raportów ad-hoc - sortowanie kolumn grupowanie, ukrywanie/odkrywanie kolumn, zaawansowane filtrowanie danych w oparciu o funkcje logiczne
-Definiowanie i zapamiętywanie własnych widoków
-Eksport danych bezpośrednio do MS Excel
-Budowa zestawień metodą drag'n'drop
-Budowa modułowa z możliwością przypisywania określonych wtyczek programu (funkcji) do poszczególnych Agentów
-Obsługa protokołu SSL zapewniającego bezpieczną komunikację Master-Serwer oraz Agent-Server.
-Połączenia pomiędzy komponentami realizowane za pomocą HTTP/HTTPS lub net.TCP
-Mechanizm kompresji pakietów danych przesyłanych przez Agenta
-Automatyczne wykrywanie lokalizacji serwera aplikacji (WS-Discovery)
-Przekazanie agentowi nowych parametrów połączenia z usługą serwera (serwer zapasowy)
-Definiowanie konfiguracji serwera proxy dla połączenia Agent-Server
-Mechanizm zdalnego pobierania bieżących aktualizacji do programu
-Help kontekstowy wraz z podręcznikiem użytkownika w polskiej wersji językowej
-Dostęp do bazy wiedzy systemu
-Definiowanie ustawień pracy Agentów (optymalizacja dla dużej liczby komputerów)
-Dedykowane narzędzie, dostarczane z systemem, do wykonywania kopii bazy danych, niezależnie od wersji silnika bazy danych (MSSQL, PostgreSQL). Uruchomienie narzędzia backupu bazy w trybie wsadowym
-Manualna i automatyczna konserwacja bazy danych - usuwanie wyników skanowania oprogramowania
-Personalizacja pakietu instalacyjnego agenta
-Określanie polityki haseł dla systemu
-Zmiana języka systemu podczas logowania
-Określenie numeru BDO przy definiowaniu rekordu firmy
-Opcja resetu hasła podczas logowania
-Globalne wyszukiwanie obiektów w systemie
-Utworzenie atrybutów jako lista/słownik
-Podgląd aktualnie zalogowanych użytkowników. Umożliwienie wylogowania wybranych użytkowników
-Definicja kalendarzy dni wolnych, uwzględnianych w module Helpdesk oraz Monitoring
-Wyszukiwarka ustawień w opcjach systemowych
-Instalacja konsoli zarządzającej w kontekście użytkownika (nie wymaga uprawnień administracyjnych)
-Historia obiektu zawiera informacje o koncie serwisowym, które wprowadziło zmianę w obiekcie
-Skanowanie lasu domen
-Budowa personalizowanego pakietu instalacyjnego
-Automatyczne zamknięcie konsoli zarządzającej po zakończeniu sesji
-Logowanie do portalu Web za pomocą mechanizmu Single Sign On

-Logowanie operacji kont serwisowych
-Dodatkowa metoda uwierzytelniania klientów przed połączeniem do serwera
-Logowanie nieudanych prób uwierzytelnienia
-Eksport danych diagnostycznych oraz dzienników operacji
-Integracja z SMS API

Dodatkowe informacje
-Kreator instalacyjny ułatwiający wdrożenie systemu
-Aplikacja dla wersji 64 bity OS
-Rozproszona architektura systemu: Serwer, konsola zarządzająca, Agent (Możliwa praca każdego z komponentów na różnych komputerach)
-Praca w oparciu o MS SQL Server oraz MS SQL Express (2008/2012/2014/2016/2019/2022 32/64 bit)
-Praca w oparciu o PostgreSQL 16 lub nowszy
-Szyfrowane połączenie pomiędzy serwerem aplikacji, a bazą danych
-Obsługa systemów operacyjnych - Agent: Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, Windows 10, Windows 11
-Obsługa systemów operacyjnych – konsola zarządzająca : Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, Windows 10, Windows 11
-Obsługa systemów operacyjnych - Serwer: Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, Windows 10, Windows 11
-Wszystkie wykonywalne komponenty systemu powinny być podpisane certyfikatem DigiCert Code Signing Certificates for Microsoft Authenticode (Digicert)
-Sterowniki systemowe powinny być podpisane certyfikatem Extended Validation (EV) Code Signing Certificate (GlobalSign) i mogą pracować w 64-bitowych systemach operacyjnych Microsoft Windows™.

Nazwy i kody zamówienia według Wspólnego Słownika Zamówień (CPV):
48517000-5 - Pakiety oprogramowania informatycznego
48730000-4 - Pakiety oprogramowania zabezpieczającego