**Opis przedmiotu zamówienia - Załącznik nr 1**

**SYSTEM DO ZARZĄDZANIA INFRASTRUKTURĄ I BEZPIECZEŃSTWEM IT eAUDITOR WEB V8 AI**

Ilość komputerów: 150

Ilość administratorów: 6

Wsparcie producenta i dostęp do aktualizacji: 24 miesiące

1. **WERSJA PODSTAWOWA SYSTEMU**

Architektura systemu

* 1. Agent – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
  2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, 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).
  3. Panel pracownika – aplikacja webowa 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.
  4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z agentami.
  5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.
  6. Komponenty Agent, konsola administracyjna, serwer, baza danych muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu.
  7. System musi umożliwiać komunikację pomiędzy agentami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.
  8. Wbudowany mechanizm automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem realizujący co najmniej: usuwanie zbędnych danych z systemu.

Wymagania systemowe

1. Konsola administracyjna działa w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, Firefox, Chrome, Opera).
2. Agent pracuje na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, 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.
3. Serwer działa na systemach 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11.
4. Serwer www jest być oparty o platformę Microsoft 64 bit (Windows Server 2012/2012R2/2016/2019/2022, Windows 10) oraz Java 8 (JRE lub JDK), Apache Tomcat 8+.
5. Baza danych działa na silniku Microsoft SQL Server 2012/2014/2016/2017/2019 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).
6. Możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.
7. Umożliwia wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej z usługi MS Active Directory.

Funkcjonalności systemu zarządzania infrastrukturą IT

* 1. Inwentaryzacja sprzętu komputerowego
  2. umożliwia automatyczną inwentaryzację komputerów z zainstalowanym agentem znajdujących się w sieci lokalnej oraz poza siecią lokalną (za NATem)
  3. zbiera szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation) oraz odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania, a także skanować  dyski twarde (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART)
  4. monitorowanie parametrów obciążenia komputerów: procesor, dyski, pamięć i sieć
  5. ewidencjonuje pliki na komputerach (nazwa, rozmiar, rodzaj, lokalizacja, w przypadku plików wykonywalnych: wersja, producent) oraz o zmiany w systemie plików (dodano plik, usunięto plik)
  6. pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów.
  7. umożliwia ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).
  8. umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja).
  9. Inwentaryzacja urządzeń podłączanych do komputera

2.1 automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.)

2.2 pozwala na przypisanie podłączonego urządzenia do komputera oraz użytkownika.

2.3 umożliwia uzyskanie informacji kto, kiedy i na jakim komputerze posługiwał się urządzeniem zewnętrznym, pozwalając na jego jednoznaczne zidentyfikowanie.

2.4 umożliwia utworzenie dowolnej ilości list urządzeń USB dozwolonych do stosowania - tzw. białe listy urządzeń USB na podstawie zdefiniowanych reguł (dozwolone/niedozwolone) wg kryteriów: użytkownik, dzień tygodnia, okres (data od, godzina od, data do, godzina do), urządzenie USB, komputer, data obowiązywania reguły.

1. Inwentaryzacja urządzeń innych niż komputery
   1. umożliwia inwentaryzację manualną dowolnych zasobów np. drukarki, switche, routery, monitory, pamięci masowe itp.
   2. posiada 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.
   3. skaner SNMP łączyć zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.
   4. zbiera informacje o jakości połączenia:

- czas odpowiedzi serwisów (usług) podawany w milisekundach: średni czas odpowiedzi, minimalny czas odpowiedzi, maksymalny czas odpowiedzi

- ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat.

* 1. wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają agenta
  2. niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci
  3. baza wzorców musi zawierać ponad 100 monitorowanych portów i usług.
  4. posiada możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci, według dowolnych filtrów użytkownika.
  5. umożliwia przypisanie urządzenia do użytkownika, ewidencję napraw, kosztów zakupu i serwisu, przypominania o upływającym terminie gwarancji oraz pozwala na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu.
  6. pozwalać na kopiowanie (duplikację) dowolnego urządzenia dowolną ilość razy.
  7. ewidencja umów utrzymaniowych (SLA) w odniesieniu do zaewidencjonowanych licencji oraz urządzeń w zakresie co najmniej: nazwa, okres, data dokumentu, numer dokumentu, dostawca, osoba kontaktowa, wartość, opis, warunki oraz umożliwiać dołączenie dowolnej ilości załączników z repozytorium i powiązanie umowy utrzymaniowej z dowolną ilością zasobów (urządzenia, licencje).
  8. Zarządzanie licencjami
  9. szczegółowe informacje o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji)
  10. ewidencja aplikacji i pakietów na komputerach oraz możliwość wykonywania audytów legalności, zdefiniowania listy aplikacji zabronionych a także zdalnego odinstalowania oprogramowania
  11. odczyt identyfikatorów i kluczy produktowych dla systemu operacyjnego oraz dowolnego oprogramowania (tam gdzie jest technicznie możliwe).
  12. wspiera następujące typy licencji: Enterprise, Licensed concurrent, Licensed Name, Licensed per Processor, Licensed per Seat, Licensed per Server, OEM, OEM Downgrade, Open, Select, MOLP Open Value (Company wide), MOLP Open Value (non-Company wide), MOLP Open Value Subscription, CAL, SAAS, Trial, Shareware, Cal Per User.
  13. umożliwia ewidencję licencji (data zakupu, cena, dostawca, nr faktury, typ licencji, klucz produktowy, identyfikator produktowy, data wygaśnięcia, nr dokumentu OT, nr zapotrzebowania) poprzez rejestrację dokumentów źródłowych (faktur zakupu) z możliwością dołączenia dowolnych załączników z repozytorium.
  14. zbiera informacje o uruchamianych aplikacjach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji, szczegóły aktywności użytkownika).

1. Zdalna administracja komputerami
   1. wykonywanie poleceń powłoki, uruchamianie aplikacji, 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
   2. skaner umożliwiający wykrywanie komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro, wersji Vpro, Serial Over LAN oraz zarządzanie komputerami z technologią Intel vPro, w tym: zdalne włączanie, wyłączanie komputera, konfiguracja BIOS, uruchomienie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji, połączenie się komputerem w trybie graficznym (od VPro v.6)
   3. za pomocą technologii Ultra VNC: zdalne podłączenie do wielu komputerów jednocześnie, przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, poprawek i aktualizacji (service pack, patch). Umożliwia podłączenia do obecnie zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejęcia dostępu)
   4. umożliwia zdefiniowanie dowolnego własnego zadania jednorazowego bądź cyklicznego z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, windows powershell oraz posiada co najmniej 70 predefiniowanych poleceń. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status)
   5. zezwala na wykonywanie zapytań WMI oraz edycję rejestrów bez zdalnego połączenia do urządzenia
   6. umożliwia wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)
   7. ewidencja logowań użytkowników do danego komputera, również w przypadku podłączania się wielu użytkowników jednocześnie, tak w sieci lokalnej, jak i poza NAT
2. Zarządzanie magazynem IT
   1. obsługa dowolnej ilości magazynów w różnych lokalizacjach
   2. obsługa dokumentów PZ, WZ, MM+, MM-, LI
   3. ewidencja materiałów w magazynach w oparciu o metodę FIFO (pierwsze przyszło pierwsze wyszło).
   4. obsługa kodów kreskowych dla materiałów w magazynach
   5. informacja o wartości materiałów w poszczególnych magazynach, aktualne stany magazynowe, dokumenty dotyczące danego materiału w dowolnym magazynie
   6. możliwość przekazania zasobu z magazynu użytkownikowi lub urządzeniu. Dokument przekazania automatycznie zapisuje się na karcie szczegółowej osoby lub urządzenia, któremu zasób został przekazany oraz w dokumentach magazynowych
3. Repozytorium
   1. możliwość dodawanie nowych dokumentów dowolnego typu, przeszukiwanie, oznaczanie dokumentów (znaczniki TAG) więcej niż jednym znacznikiem, podgląd dokumentów, dołączanie dokumentów z repozytorium w dowolnym miejscu systemu, uzyskanie informacji w jakich miejscach systemu dany dokument repozytorium występuje.
4. Kody kreskowe
   1. generowanie kodów kreskowych (jedno i dwuwymiarowych) dla każdego zaewidencjonowanego urządzenia w standardzie wybranym przez użytkownika: aztec, codabar, code128, code39, dataMatrix, EAN128, EAN13, EAN8, interleaved2of5, ITF14, PDF417, POSTNET, qrcode, royalMailCBC, UPCA, UPCE, USPSIntelligentMail.
   2. parametryzacja w zakresie wielkości graficznej kodu (wymiary, wielkość i typ czcionki)
   3. możliwość zmiany typu i atrybutów kodu w dowolnym momencie,
   4. informacja o błędzie generacji kodu, np. na skutek niewłaściwej długości wprowadzonego ciągu znaków w stosunku do danego standardu kodu.
   5. możliwość masowego wydruku kodu / kodów.
   6. obsługa kodów kreskowych nie może wymagać instalacji czcionek.
   7. umożliwia współpracę z zewnętrznymi czytnikami kodów.
5. Komunikacja za pomocą wiadomości
   1. tworzenie wiadomości tekstowych zgodne z HTML z możliwością eksportu / importu treści, celem automatycznego wysyłania do urządzeń, użytkowników lub dowolnych grup odbiorców,
   2. wiadomości wysyłane jednorazowo lub cyklicznie zgodnie z definiowalnym harmonogramem
   3. 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. użytkownik otrzymujący wiadomość jest powiadamiany wizualne i dźwiękowo
   5. wiadomości o podwyższonym priorytecie – alerty – wyświetlają się na środku ekranu, z widoczną treścią wiadomości
   6. dla wiadomości innych niż alerty użytkownik ma możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.
   7. zabezpieczenie (np. synchronizowany z serwerem znacznik czasowy) odporne na zmiany czasu na lokalnym komputerze (użytkownika) a pozwalające na jednoznaczne ustalenie daty i godziny dostarczenia i odczytania wiadomości.
   8. historia przesyłania wiadomości i odczytywania wiadomości przez użytkowników.
   9. tworzenia cyklu wiadomości szkoleniowych, dla których można wygenerować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem).
6. Monitorowanie drukarek sieciowych i wydruków
   1. posiada możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa)
   2. ewidencja wydruków obejmuje: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera z którego dokonano wydruku, format dokumentu, informację i jedno bądź dwustronnym wydruku, informację o wydruku mono/kolor.
   3. dla każdego wydruku, dla każdej drukarki oblicza rzeczywisty koszt wydruku w oparciu o wbudowany cennik wydruków obejmujący cenę papieru (w zależności od formatu) oraz cenę materiałów eksploatacyjnych (toner, tusz) dla danej drukarki, typu wydruku, rozmiaru papieru
   4. dla każdej z drukarek SNMP system musi udostępniać informacje: nr seryjny, IP, MAC, bieżący status drukarki, całkowitą ilość wydrukowanych stron, ilość wydrukowanych stron od uruchomienia, błędy, alerty, dostępne porty, stan pokryw, interfejsów sieciowych, rodzaj i ilości pamięci całkowitej i wykorzystanej, informacje o poziomie materiałów eksploatacyjnych
7. Monitorowanie stron www
   1. posiada możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej.
   2. ewidencja otwieranych stron musi dotyczyć wielu jednocześnie otwartych zakładek, również, gdy otwierana jest strona z połączeniem szyfrowanym (https) i obejmuje co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony, łączny czas korzystania, czas aktywności, czas pasywności
   3. w oparciu o algorytmy sztucznej inteligencji - machine learning oraz deep learning system umożliwia analizę treści rtcstron www oraz przypisanie im – w oparciu o treść – odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem odwiedzanych stron
   4. każda odwiedzona strona otrzymuje atrybuty: czy SSL, czy jest bezpieczna, czy zawiera przekierowania, czy znajduje się na liście CERT, czy znajduje się na liście stron hazardowych, czy kategoria strony jest bezpieczna, czy jest produktywna.
8. Worktime manager
   1. jest wyposażony w zestaw statystycznych danych o pracy użytkownika i zdefiniowanych grup użytkowników
   2. dane są prezentowane w formie interaktywnych widgetów oraz w formie danych analitycznych
   3. dane dla grup użytkowników są skumulowane oraz analityczne
   4. prezentacja danych odbywa się poprzez wskazanie pracownika lub grupy pracowników oraz wybranie okresu danych źródłowych
   5. umożliwia wyświetlanie informacji o użytkowniku pobranych z Active Directory. Informacje są aktualizowane zgodnie z harmonogramem połączenia z domeną.
   6. prezentuje w formie tabelarycznej informacje o dokumentach (np. protokoły przekazania i zwrotu sprzętu), komputerach i urządzeniach, które zostały przypisane użytkownikowi
   7. posiada widgety prezentujące dane w wybranym przedziale czasu: czas zalogowania – dni, czas pracy komputera – dni, aktywność w aplikacjach, produktywność w aplikacjach, produktywność w czasie pracy, czas pracy w aplikacjach, czas spędzony na stronach www wg kategorii stron, czas spędzony w aplikacjach (procesach) wg kategorii procesu, czas aktywność na stronach www, stron wydruku wg dokumentów, transfer sieciowy, czas pracy wg zalogowany/ wylogowany / uśpiony, czas aktywności w godzinach pracy.
9. Monitorowanie dziennika zdarzeń
   1. posiada możliwość monitorowania dziennika zdarzeń wszystkich komputerów
   2. ewidencja zdarzeń następuje w oparciu o definiowalną kategorię zdarzenia: critical, error, warning, info, audit failure, audit success, debug oraz typ dziennika: aplikacja, bezpieczeństwo, system
   3. pozwala na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia, musi zawierać: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia.
   4. umożliwiać monitorowanie komunikatów Syslog.
10. Repozytorium CMDB – centralna baza systemu umożliwiająca import i eksport danych zarówno poprzez API jak też za pomocą wbudowanego import/eksporta, na którą składają się:
    1. Active Directory - lista serwerów LDAP, z których są importowane i aktualizowane dane o użytkownikach. System pozwala na wprowadzanie dowolnej ilości serwerów dla różnych domen.
    2. kontenery dokumentów - grupy, do których można przypisywać zapisane w systemie dokumenty w celu sortowania.
    3. kategorie aplikacji - lista kategorii, do których przynależą wykorzystywane przez użytkowników aplikacje.
    4. budżet - zestawienie typów budżetów (kosztów) zaewidencjonowanych w systemie.
    5. komputery - lista zinwentaryzowanych komputerów, podzielonych wg typu autoryzacji. Widok rekordu zawiera szczegółowe dane dotyczące danego komputera.
    6. dokumenty - repozytorium dokumentów zapisanych w systemie.
    7. kategorie plików - lista typów plików kategoryzowanych przez system. Administrator ma możliwość zdefiniowania własnych grup, do których pliki będą przydzielane, według wpisanej maski.
    8. pliki - lista zinwentaryzowanych plików ze wszystkich komputerów.
    9. licencje - zestawienie licencji zapisanych w bazie systemu, które administrator może przypisywać do poszczególnych użytkowników.
    10. typy licencji - lista typów licencji.
    11. lokalizacje - lista zdefiniowanych lokalizacji, do których administrator może przypisać poszczególnych użytkowników. W odróżnieniu od struktury organizacyjnej dane nie są importowane z Active Directory.
    12. typy urządzeń - lista typów urządzeń
    13. urządzenia - lista urządzeń podzielonych wg typu.
    14. producenci / Dostawcy - lista producentów i dostawców.
    15. pamięć masowa - zestawienie dysków twardych z komputerów
    16. porty sieciowe - lista monitorowanych portów sieciowych
    17. usługi sieciowe - lista monitorowanych usług sieciowych
    18. udostępnione zasoby sieciowe - lista udostępnionych zasobów sieciowych.
    19. sieci - lista definiowalnych ręcznie sieci, do których administrator może ręcznie przypisywać komputery
    20. systemy operacyjne - zestawienie unikalnych systemów operacyjnych
    21. struktura org. - zestawienie struktur organizacyjnych zdefiniowanych bądź importowanych z Active Directory
    22. kategorie procesów - lista kategorii, do których będą przypisywane procesy aplikacji uruchamianych przez użytkowników. Klasyfikacja procesów odbywa się za pomocą algorytmów sztucznej inteligencji
    23. serwery - lista zinwentaryzowanych serwerów
    24. usługi - zestawienie usług działających na komputerach
    25. oprogramowanie - lista zinwentaryzowanego i monitorowanego oprogramowania
    26. pamięć masowa USB - lista urządzeń pamięci masowej USB
    27. administratorzy - lista administratorów i użytkowników systemu, z możliwością nadawania im indywidulanych uprawnień do wybranych funkcjonalności w systemie oraz danych użytkowników w ramach struktur organizacyjnych w zakresie przeglądania, edytowania, eksportowania i usuwania danych
    28. użytkownicy / pracownicy - lista pracowników
    29. kategorie WWW - lista kategorii stron WWW wykorzystywanych w procesie klasyfikacji stron internetowych. Klasyfikacja oparta o sztuczną inteligencję
    30. serwisy WWW - lista monitorowanych serwisów WWW.
11. Eksport danych
    1. możliwość wyeksportowania wybranych lub wszystkich danych do formatu xls, csv, pdf, OpenOffice calc, html, mht, xml, jpeg, png, gif, bmp.
    2. posiada raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu), wieloinstancyjność raportowania (wiele otwartych raportów jednocześnie z wielu widoków)
    3. generowanie raportu odbywa się po stronie serwera a nie klienta.
    4. generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów
    5. minimum 150 zdefiniowanych raportów dotyczących wszystkich obszarów funkcjonalnych
    6. możliwość ustalenia harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu.
12. Powiadomienia
    1. komunikaty w formie alertów w konsoli, wiadomości email wysyłanych na wybrane adresy oraz wiadomości SMS na wskazane numery telefonów
    2. możliwość tworzenia wielu komunikatów w oparciu o te same zdarzenia z określeniem innych grup obiorców lub parametrów
    3. możliwość edycji treści wysyłanych powiadomień oraz korzystania z danych umieszczonych w systemie w treści powiadomienia.
    4. minimum 30 zdefiniowanych powiadomień dotyczących: używania zasobów zakazanych (pliki erotyczne i pornograficzne), braku skanowania komputerów, brakach w licencjach, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www /aplikacjach, wygasaniu serwisu lub licencji, upływającej gwarancji, przekroczeniu wielkości bazy danych, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu sieci, nadmiernym obciążeniu sieci na komputerze, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku, wykryciu nowego oprogramowania lub jego odinstalowaniu, wykryciu niezgodność ze schematem oprogramowania, duplikatach adresów IP i MAC, dużej ilość danych wysyłanych przez dany port w switch’u, wykryciu nowych urządzeń w sieci, zmianie statusów portów w switch’u, podłączeniu niedozwolonego urządzenia USB, wykryciu zmiany w sprzęcie (WMI), błędach w dzienniku zdarzeń Windows, problemach z usługą systemu Windows
13. Automatyzacja
    1. możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące wraz z częstotliwością wykonywania danej czynności (godzina, dzień, tydzień, miesiąc).
    2. zdefiniowane czynności wykonywane są automatycznie.
    3. dostępne mechanizmy automatyzacji: wykonywanie kopii bezpieczeństwa bazy danych, identyfikacja aplikacji i pakietów, porządkowanie bazy danych / odbudowa indeksów, usuwanie nadmiarowych danych w bazie danych, usuwanie zewnętrznych plików (logów).
14. **FUNKCJE DODATKOWE**

**Skaner maszyn wirtualnych**

* + 1. Wykrywanie, inwentaryzacja i monitorowanie serwerów wirtualizacji MS Hyper-V oraz Vmware za pośrednictwem wbudowanych API

**Zdalna instalacja oprogramowania**

* + 1. możliwość utworzenia prywatnego repozytorium instalatorów (pliki msi i exe) oraz korzystania z repozytorium instalatorów zawierającgo minimum 30 aplikacji dostarczonego przez producenta oprogramowania
    2. szybkie filtrowanie i możliwość definiowania kategorii oprogramowania
    3. zbiorcza instalacja i deinstalacja wybranych aplikacji z poziomu konsoli administracyjnej
    4. możliwość samodzielnej instalacja i deinstalacja zatwierdzonych przez administratora aplikacji w kiosku w panelu pracownika
    5. administrator może zbiorczo przydzielać aplikacje poprzez wskazanie struktur organizacyjnych z poziomu CMDB – schematy pracownika.

**WEB RTC**

* + 1. możliwość zdalnego połączenia do wielu komputerów jednocześnie, podgląd i operowanie na pulpitach tych komputerów w technologii WEBRTC.
    2. za pomocą technologii WEBRTC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalację oprogramowania, poprawek i aktualizacji (service pack, patch).
    3. poprzez technologię WEBRTC zdalne zarządzanie plikami (tworzenie, kopiowanie, usuwanie, przesyłanie) i wykorzystanie wiersza poleceń (cmd) oraz powershell bez konieczności podłączenia do komputera.
    4. możliwość nagrywanie sesji połączeń WEBRTC jak i nawiązywanie komunikacji z użytkownikiem podczas sesji (czat).

**Szyfrowanie dysków wewnętrznych i zewnętrznych USB**

* + 1. identyfikuje partycje dysków twardych zaszyfrowane BitLockerem.
    2. posiada wbudowany mechanizmy do masowego zdalnego szyfrowania BitLockerem i wspiera metody XTS\_AES\_256, XTS\_AES\_128, AES\_256, AES\_128 oraz typy zabezpieczeń TPM+Pin, TPM, Passphrase
    3. ochrona danych na budowanych 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
    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.)
    5. funkcjonalność szyfrowania / deszyfrowania nie może być realizowana w oparciu o dodatkowego agenta na stacji roboczej lecz musi być integralnym rozwiązaniem oferowanego systemu.
    6. zdalne szyfrowanie / deszyfrowanie partycji systemowych oraz niesystemowych oraz prezentować w konsoli administracyjnej bieżący postęp procesu
    7. szyfrowanie partycji niesystemowych oraz USB polega na wprowadzeniu przez użytkownika hasła
    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. proces szyfrowania może być zatrzymany podczas hibernacji oraz wyłączenia systemu ale jest kontynuowany po wzbudzeniu / włączeniu komputera.
    10. system przechowuje klucze szyfrujące w konsoli administracyjnej, przy czym klucze są dostępne po dodatkowym uwierzytelnieniu administratora.
    11. umożliwia szyfrowanie / deszyfrowanie komputerów w sieci lokalnej oraz poza NATem.

Monitorowanie uprawnień ACL

* + 1. umożliwia skanowanie list kontroli dostępu (ang., tzw. access-control list, ACL) z systemu katalogowego komputerów lokalnych oraz serwerów.
    2. dane muszą zawierać: nazwę komputera, ścieżkę, właściciela folderu, nazwę grupy uprawnień, listę nadanych uprawnień, datę aktualizacji.
    3. odczyt uprawnień na serwerach musi następować zgodnie ze zdefiniowanym harmonogramem.
    4. posiada predefiniowane filtry pozwalające na filtrowanie uprawnień do zasobów lokalnych oraz współdzielonych.
    5. dane są prezentowane w układach: Foldery -> Użytkownicy, Użytkownicy -> Foldery, Grupy -> Foldery, Właściciele -> Foldery.
    6. posiada minimum trzy predefiniowane raporty prezentujące informacje zebrane podczas skanowania uprawnień.

System wsparcia technicznego eHelpDesk

* + 1. pomoc administratorom w obsłudze zgłoszeń problemów zgłoszonych przez użytkowników
    2. integralna cześć systemu do zarządzania zasobami IT tego samego producenta.
    3. interfejs użytkownikaumożliwiający generowanie zgłoszeń serwisowych z poziomu panelu pracownika, sprawdzanie ich statusu oraz dodaniu notatek widocznych dla serwisanta
    4. interfejs serwisantaumożliwia dokładną rejestrację i klasyfikację zgłoszeń oraz tworzenie dowolnych kategorii zgłoszenia

automatycznie zapisuje się pełna historię zgłoszenia

* + 1. możliwość automatycznego wysłania powiadomień e-mail o wszelkich zdarzeniach dotyczących zgłoszenia do zdefiniowanych użytkowników
    2. Licencja dla 6 administratorów.