



## Opis przedmiotu zamówienia

### Narzędzia do monitorowania i zarządzania infrastrukturą sieciową – Urząd Gminy, 30 licencji

Lp.	Minimalne wymagania techniczne oprogramowania
1	<p>Oprogramowanie musi posiadać budowę modułową, składać się z serwera zarządzającego, zdalnych konsoli oraz agentów. Komunikacja pomiędzy serwerem a agentami i konsolami powinna być nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. Program musi umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą.</p> <p>Moduły musi umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program musi wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12 – lub równoważny) dzięki czemu nie jest objęty limitem ilości danych, baza danych jest rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. instalacja serwera oraz konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows. – lub równoważny</p> <p>Dane, które dotyczą działań pracownika na komputerze: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., muszą być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej muszą być przez system grupowane w osobnym, dedykowanym oknie. Oprogramowanie musi mieć możliwość, zgodnie z obowiązującymi przepisami o ochronie danych osobowych RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.</p> <p>Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych Administratorów</p> <p>Oprogramowanie musi posiadać możliwość nadawania kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny</p>



	<p>Administrator musi mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną, m.in. musi móc wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Działania administratorów muszą być logowane oznacza to, że program musi posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog. Oprogramowanie musi mieć możliwość synchronizacji z Active Directory, również przez szyfrowane połączenie LDAPS listy kont użytkowników, w tym administratorów.</p> <p>Program musi umożliwiać konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityki muszą pozawalać na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymuszać dostosowanie bieżących haseł do obowiązujących zasad.</p> <p>Program musi mieć możliwość implementacji na minimum 40 (30 + 10) urządzeniach jednocześnie.</p> <p>Program musi zawierać mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny może być wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA musi być możliwość skonfigurowania okresu, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania może być pominięta tylko w lokalnej konsoli serwera.</p> <p>Producent oprogramowania musi posiadać znak jakości CYBERSECURITY MADE IN EUROPE przyznawanym przez Europejską Organizację ds. Cyberbezpieczeństwa (ECSO). – lub równoważne</p>
2	<p><b>Moduł monitorowania aktywności użytkowników w programie musi posiadać następujące funkcjonalności:</b></p> <p>Monitorowanie Aktywności Użytkowników</p> <p>Czas Aktywności:</p> <p>Rejestracja dokładnego czasu pracy użytkownika, w tym godziny rozpoczęcia i zakończenia pracy.</p>



#### Monitorowanie Procesów:

Śledzenie każdego procesu z podziałem na całkowity czas działania oraz czas aktywności użytkownika.

Informowanie o procesach uruchomionych z podwyższonymi uprawnieniami.

#### Użycie Programów:

Procentowa analiza wykorzystania aplikacji względem całkowitego czasu jej działania.

Informacje o komputerze, na którym wykonano daną aktywność.

#### Dokumenty:

Rejestrowanie informacji o edytowanych przez użytkownika dokumentach.

#### Historia Pracy:

Cykliczne zrzuty ekranowe z aktywności użytkownika.

#### Odwiedzane Strony WWW:

Lista odwiedzanych stron wraz z tytułami, adresami, liczbą i czasem wizyt.

#### Transfer Sieciowy:

Monitorowanie ruchu sieciowego, zarówno lokalnego, jak i internetowego generowanego przez użytkownika.

#### Wydruki:

Informacje o dacie wydruku, wykorzystaniu drukarek, raporty dla każdego użytkownika, w tym kiedy, ile stron, na jakiej drukarce i jaki dokument był drukowany.

Możliwość grupowania drukarek i monitorowania kosztów wydruków.



E-maile:

Rejestrowanie nagłówków przesyłanych wiadomości e-mail w aplikacjach klienckich.

Dodatkowe Funkcjonalności

Wykrywanie Podejrzanej Aktywności:

Detekcja aktywności symulowanej przez popularne „jiggler” (symulowanie pracy).

Wykrywanie symulowanej aktywności (min. 15 minut) poprzez ruch myszą bez kliknięcia lub ciągle wprowadzanie tego samego znaku.

Wyszczególnienie podejrzanej aktywności w raportach, generowanie alarmów oraz automatyczne włączanie zapisywania zrzutów ekranowych po wykryciu.

Blokowanie Stron WWW:

Możliwość blokowania całego ruchu WWW dla stacji roboczej użytkownika, z definiowaniem wyjątków (dozwolone i zabronione domeny oraz sub-domeny).

Integracja list stron z plików .TXT z zewnętrznych źródeł np. CERT.

Wbudowana lista stron sklasyfikowanych jako zagrożenia i automatyczne odświeżanie list z zewnętrznych źródeł.

Blokowanie Ruchu i Plików:

Blokowanie ruchu na wybranych portach TCP/IP.

Blokowanie pobierania plików z określonymi rozszerzeniami poprzez przeglądarki internetowe.

Rejestr Naruszeń:

Prowadzenie rejestru naruszeń blokad.

Powiadomienia:

Wysyłanie powiadomień o odwiedzaniu stron z określonych grup domen, transferze danych, wydrukach oraz naruszeniach blokad.



	<p>Raporty i Metryki:</p> <p>Generowanie raportów z ustawieniami monitorowania użytkownika, które można dołączyć np. do akt pracownika.</p> <p>Definiowanie Czasu Monitorowania:</p> <p>Ustalanie godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.</p>
3	<p><b>Moduł monitorowania infrastruktury musi posiadać następujące funkcjonalności:</b></p> <p>Wykrywanie i Wizualizacja Urzędzeń</p> <p>Wykrywanie Urzędzeń w Sieci:</p> <p>Wykrywanie urządzeń w sieci poprzez skanowanie ping oraz arp-ping.</p> <p>Wykrywanie urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU).</p> <p>Wizualizacja Urzędzeń na Mapach:</p> <p>Wizualizacja stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci.</p> <p>Wizualizacja urządzeń na mapach z funkcją siatki umożliwiającą korygowanie pozycji ikon na mapie do najbliższej linii siatki.</p> <p>Wizualizacja map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.</p> <p>Wizualizacja map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków (np. schematu rozmieszczenia pomieszczeń w budynku).</p> <p>Wizualizacja map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze.</p> <p>Wizualizacja map urządzeń poprzez wstawianie dowolnego tekstu na mapie.</p>



Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji o podłączonych portach przełącznika, zarówno manualnie jak i automatycznie.

Zablokowanie mapy urządzeń przed przypadkową edycją.

#### Monitorowanie Serwisów i Systemów

##### Monitorowanie Serwisów TCP/IP i Innych:

Monitorowanie serwisów TCP/IP, HTTP, POP3, SMTP, FTP oraz możliwość definiowania własnych serwisów.

Monitorowanie czasu odpowiedzi serwisów i procentu utraconych pakietów.

##### Monitorowanie Serwerów Poczty:

Monitorowanie czasu logowania do serwisu odbierającego oraz czasu wysyłania poczty.

Możliwość monitorowania stanu systemów i wysyłania powiadomień (e-mail, SMS i inne) w przypadku ich nieodpowiedniego funkcjonowania.

Możliwość wykonywania operacji testowych.

Wysyłanie powiadomień w przypadku awarii serwera pocztowego.

##### Monitorowanie Stron WWW i Bezpieczeństwo

##### Monitorowanie Serwerów WWW i Adresów URL:

Cykliczne monitorowanie czasu ładowania strony internetowej, zmiany treści na stronie oraz statusu protokołu HTTPS.

Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail.

##### Obsługa Urządzeń SNMP i Syslog

##### Obsługa Urządzeń SNMP:

Monitorowanie urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP).



Monitorowanie wartości za pomocą nazw zmiennych oraz OID.

Obsługa Komunikatów Syslog i Pułapek SNMP:

Ewidencjonowanie odebranych danych z komunikatów syslog i pułapek SNMP.

Monitorowanie Routerów i Przełączników:

Monitorowanie zmian stanu interfejsów sieciowych.

Monitorowanie ruchu sieciowego.

Monitorowanie podłączonych stacji roboczych oraz graficzna prezentacja panelu switcha.

Monitorowanie ruchu generowanego przez podłączone do portów stacje robocze.

Monitorowanie Serwisów Windows – lub równoważne:

Monitorowanie serwisów Windows oraz równoważnych, alarmowanie w przypadku zatrzymania serwisu oraz możliwość jego uruchomienia, zatrzymania lub zrestartowania.

Integracja i Powiadomienia

Integracja z Bramką GSM:

Możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

Dodatkowe Funkcje Monitoringu

Wykonywanie Operacji Testowych:

Możliwość wykonywania operacji testowych dla monitorowanych serwisów i systemów.

Powiadomienia o Awariach:

Wysyłanie powiadomień (e-mail, SMS, inne) w razie nieodpowiedniego funkcjonowania serwisów lub systemów, np. gdy ważne parametry znajdują się poza zakresem.



4

**Moduł inwentaryzacyjny musi posiadać następujące funkcjonalności:**

Automatyzacja i Monitorowanie

Automatyczne Gromadzenie Danych: Automatyczne gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych.

Szczegóły Sprzętu:

Prezentowanie szczegółów dotyczących sprzętu, takich jak model, procesor, pamięć, płyta główna, napędy, karty itp.

Odczyt Parametrów S.M.A.R.T.:

Odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.

Zestawienia Konfiguracji:

Zestawienia posiadanych konfiguracji sprzętowych, wolnego miejsca na dyskach, średniego wykorzystania pamięci, oraz informacji pozwalających na wytypowanie systemów wymagających upgrade'u.

Informacja o Aplikacjach:

Informowanie o zainstalowanych aplikacjach oraz aktualizacjach Windows – lub równoważne, umożliwiające audytowanie i weryfikację użytkowania licencji w organizacji.

Powiadomienia i Zarządzanie

Powiadomienia o Zmianach: Możliwość wysyłania powiadomień (np. e-mailem) w przypadku zainstalowania programu lub zmiany konfiguracji sprzętowej komputera.

Odczyt Numeru Seryjnego:

Możliwość odczytania numeru seryjnego (klucze licencyjne).

Automatyczne Zarządzanie Oprogramowaniem: Automatyczne





zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.

#### Przegląd Konfiguracji Systemu:

Przegląd informacji o konfiguracji systemu, takich jak komendy startowe, zmienne środowiskowe, konta lokalnych użytkowników, harmonogram zadań itp.

#### Zarządzanie Plikami Użytkowników:

Utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika.

#### Integracja i Zarządzanie Zasobami

#### Wymiana Plików:

Możliwość wymiany plików do i ze stacją roboczą poprzez funkcję Menedżera plików, z logowaniem działań administratorów.

#### Baza Ewidencji Majątku IT:

Przechowywanie informacji o infrastrukturze IT w jednym miejscu z automatycznym aktualizowaniem danych.

Przydzielanie dostępu administratorów do zasobów na podstawie praw do oddziałów.

Tworzenie powiązań między zasobami a urządzeniami oraz kontami użytkowników (lokalnymi i zsynchronizowanymi z Active Directory).

Definiowanie własnych typów zasobów, ich atrybutów oraz wartości.

Masowa edycja atrybutów zasobów.

Import danych z zewnętrznego źródła (.CSV).

Przechowywanie dokumentów (np. skan faktury zakupu, gwarancji).



## Zarządzanie i Audyt Licencji

### Pozyskiwanie Informacji o Oprogramowaniu:

Skanowanie plików wykonywalnych i multimedialnych, oraz archiwów ZIP na stacjach roboczych.

Informacje o aplikacjach używanych w organizacji.

Tworzenie własnych wzorców aplikacji i kategorii aplikacji.

Informacje o komputerach, na których aplikacja została wykryta.

### Zarządzanie Licencjami:

Zarządzanie posiadanymi licencjami, wskazywanie osób odpowiedzialnych i użytkowników licencji.

Tworzenie powiązań między licencjami a dokumentami w relacji 1:N.

Audyt legalności oprogramowania i powiadamianie w razie przekroczenia liczby posiadanych licencji.

Generowanie raportów zgodności licencji.

### Dodatkowe Funkcje

#### Okna Audytowe:

Możliwość filtrowania elementów per oddział.

#### Tworzenie Kodów Kreskowych:

Tworzenie i drukowanie kodów kreskowych oraz QR Code dla zasobów z numerem inwentarzowym.



	<p>Inwentaryzacja Mobilna: Inwentaryzacja zasobów za pomocą aplikacji mobilnej dla systemu Android.</p> <p>Alarmy i Powiadomienia: Definiowanie alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data”.</p>
5	<p>Moduł zdalnej pomocy użytkownikom w programie powinien zawierać następujące funkcjonalności:</p> <p>Zdalne Zarządzanie i Kontrola</p> <p>Podgląd i Kontrola Pulpitu:</p> <p>Podgląd pulpitu użytkownika z możliwością przejęcia nad nim kontroli.</p> <p>Definiowanie, czy użytkownik powinien zostać zapytany o zgodę na połączenie oraz możliwość odrzucenia połączenia (np. dla pracowników wysokiego szczebla).</p> <p>Podczas zdalnego dostępu, zarówno użytkownik, jak i administrator widzą ten sam ekran.</p> <p>Możliwość wyboru dowolnego ekranu (monitora) oraz blokowania działania myszy i klawiatury dla użytkownika.</p> <p>Równoczesne podłączenie do tego samego komputera przez kilku administratorów.</p> <p>System Zgłoszeń i Portal HelpDesk</p> <p>Baza Zgłoszeń:</p> <p>Umożliwia użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal i e-mail.</p>



Automatyczne przyporządkowanie zgłoszeń odpowiednim administratorom z powiadomieniem.

Integracja ze skrzynkami e-mail poprzez klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. – lub równoważnym

Przetwarzanie zgłoszeń w trybie anonimowym zgodnie z "Dyrektywą o sygnalistach".

Dokumenty prawne dot. ochrony sygnalistów i szablon regulaminu zgłoszeń wewnętrznych.

Monitorowanie Procesu Rozwiązywania Zgłoszeń:

Użytkownicy mogą monitorować statusy zgłoszeń i wymieniać informacje z administratorem poprzez komentarze.

Możliwość użycia pośredniego statusu „zgłoszenie rozwiązane” przed ostatecznym zamknięciem zgłoszenia.

Czat:

Rozmowy w czasie rzeczywistym i archiwizacja historii wiadomości.

Zarządzanie dostępem do czatu na 3 poziomach: pełny dostęp, brak dostępu, dostęp ograniczony do pomocy technicznej.

Rozmowy między „zwykłymi” użytkownikami.

Przesyłanie plików, tworzenie pokoi tematycznych i rozmów grupowych.

Oznaczanie kontaktów jako „ulubionych”.



Dostępność z ikony Agenta i interfejsu WWW HelpDesku, tryb jasny/ciemny.

Baza Wiedzy i Komunikaty

Baza Wiedzy:

Pomoc w samodzielnym rozwiązywaniu problemów z nadawaniem artykułom statusów (opublikowany, wewnętrzny, szkic).

Informowanie o zdarzeniach (np. planowanych przestojach) poprzez komunikaty z graficznym formatowaniem treści i łączami do artykułów.

Historia odczytanych komunikatów dostępna z poziomu ikony Agenta.

Tworzenie szkiców i archiwizowanie komunikatów.

Dostęp Zdalny:

Możliwość dostępu z prywatnego komputera do komputera firmowego za pomocą funkcji zdalnego dostępu.

Zarządzanie Użytkownikami i Kontami

Integracja z Active Directory:

Pobieranie listy użytkowników z Active Directory.

Wyświetlanie wizytówek użytkowników w systemie zgłoszeń.

Zarządzanie Kontami Windows – lub równoważne:



Tworzenie, usuwanie, aktywacja, edycja uprawnień, reset haseł, edycja kont.

Zarządzanie Dostępem i Zgłoszeniami:

Zarządzanie dostępem do zgłoszeń dla pracowników HelpDesku i użytkowników końcowych.

Tworzenie drzewa kategorii zgłoszeń do 4 poziomów, opisy kategorii, klauzule RODO.

Automatyczne przypisywanie zgłoszeń do pracowników HelpDesku.

Definiowanie ścieżek akceptacji zgłoszeń.

Eksportowanie listy zgłoszeń do plików CSV i XLSX.

Formularze i Operacje Zgłoszeń:

Tworzenie formularzy z niestandardowymi polami opisowymi.

Operacje na wielu zgłoszeniach równocześnie.

Dołączanie załączników do zgłoszeń.

Wyszukiwanie zgłoszeń i artykułów w bazie wiedzy.

Komentarze i czas poświęcony na rozwiązanie przy zamykaniu zgłoszenia.

Dystrybucja Oprogramowania i Zdalne Operacje

Dystrybucja Oprogramowania:



Dystrybucja oprogramowania przez Agenty.

Definiowanie aplikacji do samodzielnej instalacji przez użytkowników z pakietów MSI. – lub równoważnych

Kolejkowanie zadań dystrybucji plików.

Automatyzacja Procesów Zgłoszeń:

Konfiguracja automatyzacji z powiadomieniami e-mail.

Dodawanie komentarzy publicznych z załącznikami i odnośnikami do artykułów w Bazie Wiedzy.

Zarządzanie Procesami Windows – lub równoważne:

Zakończenie procesów, uruchamianie nowych procesów w sesji użytkownika.

Menedżer Plików:

Wymiana plików do i ze stacji roboczej bez blokowania interfejsu programu podczas przesyłania.

Raporty i Obsługa SLA

Planowanie Nieobecności HelpDesk:

Zarządzanie nieobecnościami pracowników HelpDesku.

Obsługa SLA:



	<p>Monitorowanie umów o gwarantowanym poziomie świadczenia usług (SLA).</p> <p>Generowanie raportów przekroczeń SLA i podsumowań.</p> <p>Generowanie Raportów:</p> <p>Tworzenie raportów obsługi helpdesk.</p>
6	<p>Moduł ochrony danych przed wyciekiem poprzez blokowanie urządzeń w programie powinien zawierać następujące funkcjonalności:</p> <p>Blokowanie Urządzeń i Nośników Danych</p> <p>Zarządzanie Prawami Dostępu:</p> <p>Kontrola dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.</p> <p>Blokowanie Urządzeń i Interfejsów Fizycznych:</p> <p>Blokowanie urządzeń i interfejsów takich jak: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.</p> <p>Blokowanie Interfejsów Bezprzewodowych:</p> <p>Blokowanie interfejsów bezprzewodowych, w tym Wi-Fi, Bluetooth, IrDA.</p> <p>Blokowanie Urządzeń do Przenoszenia Danych:</p> <p>Blokowanie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.</p>





#### Alarmowanie o Zdarzeniach:

Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych z możliwością ograniczenia alarmów tylko do nośników niezaufanych.

#### Funkcje Wspierające Bezpieczeństwo Systemu

Integracja z Windows Defender - lub równoważne:

Zarządzanie ustawieniami Windows Defender – lub równoważny, w tym odczyt stanu ochrony, włączanie i wyłączanie ochrony, tworzenie reguł ruchu.

Monitorowanie Stanu Szyfrowania Dysków:

Monitorowanie stanu szyfrowania dysków za pomocą BitLocker. – lub równoważny

Zdalne Szyfrowanie Dysków:

Zdalne szyfrowanie dysków za pomocą BitLocker – lub równoważny oraz zapisywanie klucza odzyskiwania do pliku i jako zasób w bazie danych programu.

Odczyt Aktywnego Oprogramowania Antywirusowego:

Odczyt informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender. – lub równoważny

Monitorowanie Stanu Modułu TPM:

Monitorowanie stanu modułu TPM (Trusted Platform Module).



## Zarządzanie Prawami Dostępu do Urządzeń

### Definiowanie Praw Użytkowników/Grup:

Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.

### Autoryzowanie Urządzeń Firmowych:

Autoryzowanie firmowych urządzeń, np. szyfrowanych pendrive'ów i dysków, blokowanie urządzeń prywatnych.

### Blokowanie Typów Urządzeń:

Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.

### Centralna Konfiguracja Reguł:

Centralna konfiguracja reguł (polityk) dla całej sieci.

### Usuwanie Znanych Urządzeń:

Usuwanie z listy znanych urządzeń tych, które zostały zutylizowane.

### Audyt Operacji na Plikach na Urządzeniach Przenośnych

### Zapisywanie Informacji o Zmianach w Systemie Plików:

Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.

### Monitorowanie Operacji na Plikach:



Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika oraz na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.).

Te funkcjonalności zapewniają kompleksową ochronę danych przed wyciekiem poprzez kontrolę dostępu do urządzeń, monitorowanie operacji na plikach oraz integrację z systemami bezpieczeństwa, co znacząco zwiększa bezpieczeństwo danych w organizacji.

Moduł wspierający zarządzanie czasem i analizowanie aktywności użytkowników w programie powinien zawierać następujące funkcjonalności:

Funkcje Zarządzania Czasem i Aktywnością Użytkowników

Statystyki Czasu Pracy i Aktywności Prywatnej:

Dostarczanie informacji o czasie poświęconym na pracę oraz aktywności prywatnej w wybranym przedziale czasu. Użytkownicy mogą oznaczać sesje aktywności jako czas prywatny.

Dostęp do Wskaźników Aktywności:

Użytkownicy mogą przeglądać swoje wskaźniki aktywności w czasie pracy oraz przeglądać historyczne dane z dowolnego okresu.

Dostęp Menedżerów i Przełożonych:

Menedżerowie i przełożeni mają automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie, co pozwala na analizę i identyfikację obszarów wymagających największego zaangażowania.

Statystyki Aktywności Grup i Podwładnych:



Statystyki aktywności grupy i jej członków są widoczne dla menedżera grupy, a statystyki aktywności podwładnych dla przełożonego.

Lista Odwiedzanych Stron i Aplikacji:

Lista odwiedzanych stron internetowych i używanych aplikacji wraz ze spędzonym na nich czasem.

Podgląd Użytkowników Korzystających z Aplikacji:

Możliwość podglądu listy użytkowników korzystających z wybranej aplikacji w określonym czasie.

Statystyki Popularności:

Statystyki popularności stron i aplikacji w organizacji, grupie oraz u poszczególnych użytkowników.

Ocena Produktyności:

Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.

Grupowanie Stron i Aplikacji:

Grupowanie stron internetowych i aplikacji na kategorie: produktywne, neutralne i nieproduktywne.

Przypisywanie Wyjątków Produktyności:

Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne.



Edycja Klasyfikacji Aplikacji:

Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).

Wskaźnik Czasu Aktywności Produktywnej:

Wskaźnik czasu poświęconego na aktywność produktywną.

Definiowanie Progu Produktywności:

Definiowanie wymaganego progu produktywności i limitu nieproduktywności z możliwością włączenia dla nich alarmów e-mail.

Przypisywanie Kategorii Aplikacjom i Stronom:

Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka, z możliwością edycji predefiniowanej listy kategorii.

Lista Kontaktów w Organizacji:

Lista kontaktów z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.

Portal Informacyjny w Formie Platformy WWW

Oprogramowanie posiada również portal informacyjny w formie platformy WWW, który pozwala na tworzenie interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami. Każdy widget można dostosować i nazwać wg potrzeb.

Zarządzanie Panelami Informacyjnymi:



	<p>Widżety są rozmieszczane na siatce o ustalonym przez administratora rozmiarze, a zawartość paneli jest automatycznie odświeżana.</p> <p>Udostępnianie Paneli:</p> <p>Panele mogą być udostępniane w trybie „tylko do odczytu” z zabezpieczeniem tokenem.</p> <p>Tryb Jasny i Ciemny:</p> <p>Możliwość wyświetlania portalu w trybie jasnym lub ciemnym (nocnym).</p> <p>Zarządzanie Uprawnieniami:</p> <p>Zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego.</p> <p>Prezentacja Danych z Modułów:</p> <p>Widżety prezentują dane z różnych modułów funkcjonalnych, takich jak:</p> <p>Mapa sieci, Liczniki wydajności, alarmy i odpowiedzi serwisów TCP/IP, Zmiany w konfiguracji sprzętowej i aplikacyjnej urządzeń z Agentami, Statystyki wydruków, użycia aplikacji, aktywności WWW, naruszenia reguł blokad, Statystyki obsługi zgłoszeń, lista najnowszych i najstarszych nierozwiązanych zgłoszeń, zgłoszenia z naruszonym SLA, Informacje o stanie BitLocker, Windows Defender, Windows Firewall, Produktywność grupy, statystyki czasu nieproduktywnego. – lub równoważne</p>
7	<p>Moduł ochrony danych przed wyciekiem poprzez blokowanie urządzeń w programie powinien zawierać następujące funkcjonalności:</p> <p>Blokowanie Urządzeń i Nośników Danych</p> <p>Zarządzanie Prawami Dostępu:</p>



Kontrola dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.

Blokowanie Urządzeń i Interfejsów Fizycznych:

Blokowanie urządzeń i interfejsów takich jak:

USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.

Blokowanie Interfejsów Bezprzewodowych:

Blokowanie interfejsów bezprzewodowych, w tym Wi-Fi, Bluetooth, IrDA.

Blokowanie Urządzeń do Przenoszenia Danych:

Blokowanie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.

Alarmowanie o Zdarzeniach:

Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych z możliwością ograniczenia alarmów tylko do nośników niezauważalnych.

Funkcje Wspierające Bezpieczeństwo Systemu

Integracja z Windows Defender – lub równoważne:

Zarządzanie ustawieniami Windows Defender, - lub równoważne w tym odczyt stanu ochrony, włączanie i wyłączanie ochrony, tworzenie reguł ruchu.

Monitorowanie Stanu Szyfrowania Dysków:



Monitorowanie stanu szyfrowania dysków za pomocą BitLocker. – lub równoważny

Zdalne Szyfrowanie Dysków:

Zdalne szyfrowanie dysków za pomocą BitLocker – lub równoważne oraz zapisywanie klucza odzyskiwania do pliku i jako zasób w bazie danych programu.

Odczyt Aktywnego Oprogramowania Antywirusowego:

Odczyt informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender. – lub równoważne

Monitorowanie Stanu Modułu TPM:

Monitorowanie stanu modułu TPM (Trusted Platform Module).

Zarządzanie Prawami Dostępu do Urządzeń

Definiowanie Praw Użytkowników/Grup:

Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.

Autoryzowanie Urządzeń Firmowych:

Autoryzowanie firmowych urządzeń, np. szyfrowanych pendrive'ów i dysków, blokowanie urządzeń prywatnych.

Blokowanie Typów Urządzeń:

Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.





Centralna Konfiguracja Reguł:

Centralna konfiguracja reguł (polityk) dla całej sieci.

Usuwanie Znanych Urządzeń:

Usuwanie z listy znanych urządzeń tych, które zostały zutylizowane.

Audyt Operacji na Plikach na Urządzeniach Przenośnych

Zapisywanie Informacji o Zmianach w Systemie Plików:

Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.

Monitorowanie Operacji na Plikach:

Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika oraz na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.).

Te funkcjonalności zapewniają kompleksową ochronę danych przed wyciekiem poprzez kontrolę dostępu do urządzeń, monitorowanie operacji na plikach oraz integrację z systemami bezpieczeństwa, co znacząco zwiększa bezpieczeństwo danych w organizacji.

Moduł wspierający zarządzanie czasem i analizowanie aktywności użytkowników w programie powinien zawierać następujące funkcjonalności:

Funkcje Zarządzania Czasem i Aktywnością Użytkowników

Statystyki Czasu Pracy i Aktywności Prywatnej:



Dostarczanie informacji o czasie poświęconym na pracę oraz aktywności prywatnej w wybranym przedziale czasu. Użytkownicy mogą oznaczać sesje aktywności jako czas prywatny.

Dostęp do Wskaźników Aktywności:

Użytkownicy mogą przeglądać swoje wskaźniki aktywności w czasie pracy oraz przeglądać historyczne dane z dowolnego okresu.

Dostęp Menedżerów i Przełożonych:

Menedżerowie i przełożeni mają automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie, co pozwala na analizę i identyfikację obszarów wymagających największego zaangażowania.

Statystyki Aktywności Grup i Podwładnych:

Statystyki aktywności grupy i jej członków są widoczne dla menedżera grupy, a statystyki aktywności podwładnych dla przełożonego.

Lista Odwiedzanych Stron i Aplikacji:

Lista odwiedzanych stron internetowych i używanych aplikacji wraz ze spędzonym na nich czasem.

Podgląd Użytkowników Korzystających z Aplikacji:

Możliwość podglądu listy użytkowników korzystających z wybranej aplikacji w określonym czasie.

Statystyki Popularności:

Statystyki popularności stron i aplikacji w organizacji, grupie oraz u poszczególnych użytkowników.



#### Ocena Produktivności:

Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.

#### Grupowanie Stron i Aplikacji:

Grupowanie stron internetowych i aplikacji na kategorie: produktywne, neutralne i nieproduktywne.

#### Przypisywanie Wyjątków Produktivności:

Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne.

#### Edycja Klasyfikacji Aplikacji:

Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).

#### Wskaźnik Czasu Aktywności Produktivnej:

Wskaźnik czasu poświęconego na aktywność produktywną.

#### Definiowanie Progu Produktivności:

Definiowanie wymaganego progu produktywności i limitu nieproduktywności z możliwością włączenia dla nich alarmów e-mail.

#### Przypisywanie Kategorii Aplikacjom i Stronom:



Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka, z możliwością edycji predefiniowanej listy kategorii.

Lista Kontaktów w Organizacji:

Lista kontaktów z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.

Portal Informacyjny w Formie Platformy WWW

Oprogramowanie posiada również portal informacyjny w formie platformy WWW, który pozwala na tworzenie interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami. Każdy widget można dostosować i nazwać wg potrzeb.

Zarządzanie Panelami Informacyjnymi:

Widgety są rozmieszczane na siatce o ustalonym przez administratora rozmiarze, a zawartość paneli jest automatycznie odświeżana.

Udostępnianie Paneli:

Panele mogą być udostępniane w trybie „tylko do odczytu” z zabezpieczeniem tokenem.

Tryb Jasny i Ciemny:

Możliwość wyświetlania portalu w trybie jasnym lub ciemnym (nocnym).

Zarządzanie Uprawnieniami:

Zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego.



	<p>Prezentacja Danych z Modułów:</p> <p>Widżety prezentują dane z różnych modułów funkcjonalnych, takich jak:</p> <p>Mapa sieci, Liczniki wydajności, alarmy i odpowiedzi serwisów TCP/IP, Zmiany w konfiguracji sprzętowej i aplikacyjnej urządzeń z Agentami, Statystyki wydruków, użycia aplikacji, aktywności WWW, naruszenia reguł blokad, Statystyki obsługi zgłoszeń, lista najnowszych i najstarszych nierozwiązanych zgłoszeń, zgłoszenia z naruszonym SLA, Informacje o stanie BitLocker, Windows Defender, Windows Firewall – lub równoważne, Produktywność grupy, statystyki czasu nieproduktywnego.</p>
8.	<p>Wdrożenie oraz szkolenie z Administracji i Zarządzania Systemami Monitoringu IT</p> <p>1. Wprowadzenie:</p> <p>Wprowadzenie, cele i oczekiwania.</p> <p>2. Sieć:</p> <p>Co to właściwie są liczniki wydajności?</p> <p>Wprowadzenie do koncepcji liczników wydajności sieciowej.</p> <p>Metryki wydajności i ich znaczenie w zarządzaniu siecią.</p> <p>Co ciekawego można otrzymać monitorując bez agenta?</p> <p>Techniki monitorowania sieci bez użycia agentów.</p> <p>Analiza ruchu sieciowego i identyfikacja problemów.</p> <p>Zbieranie logów.</p> <p>Procesy i metody zbierania logów z urządzeń sieciowych.</p> <p>Przegląd narzędzi do zbierania logów.</p> <p>Wysyłanie logów.</p> <p>Konfiguracja i zarządzanie przesyłaniem logów do centralnych systemów monitoringu.</p> <p>Integracja z systemami SIEM.</p> <p>Alarmowanie.</p>



Ustawianie alarmów i powiadomień na podstawie zebranych logów.

Przykłady scenariuszy alarmowania i reagowania.

### 3. Inwentarz:

Jak systemy monitoringu wykrywają aplikacje?

Mechanizmy automatycznego wykrywania aplikacji.

Identyfikacja i klasyfikacja zasobów programowych.

Rozliczanie licencji.

Monitorowanie i zarządzanie licencjami oprogramowania.

Narzędzia do automatycznego śledzenia zgodności licencyjnej.

Sprzęt vs. zasoby.

Inwentaryzacja sprzętu i zarządzanie zasobami fizycznymi.

Przegląd narzędzi do zarządzania inwentarzem IT.

Praca z zasobami.

Zarządzanie cyklem życia zasobów IT.

Optymalizacja wykorzystania zasobów w organizacji.

### 4. Użytkownicy:

Podjęta aktywność.

Identyfikacja i analiza podejrzanych działań użytkowników.

Narzędzia do monitorowania aktywności użytkowników.

Zrzuty ekranów.

Tworzenie i zarządzanie zrzutami ekranów użytkowników.

Zastosowania zrzutów w analizie bezpieczeństwa.

Blokady.

Implementacja mechanizmów blokowania użytkowników.

Procedury blokowania i odblokowywania dostępu.

Alarmy naruszeń.

Konfiguracja alarmów na podstawie naruszeń polityk bezpieczeństwa.



Przykłady zastosowań alarmów w systemach IT.

#### 5. Ochrona Danych:

Monitorowanie operacji na plikach.

Śledzenie i rejestrowanie operacji na plikach i folderach.

Analiza logów operacji plikowych.

Zarządzanie nośnikami.

Zarządzanie fizycznymi i wirtualnymi nośnikami danych.

Polityki bezpieczeństwa dla nośników danych.

Szyfrowanie komputerów.

Implementacja i zarządzanie szyfrowaniem dysków i komputerów.

Przegląd technologii szyfrowania i najlepsze praktyki.

Alarmy.

Ustawianie alarmów związanych z bezpieczeństwem danych.

Monitorowanie i reagowanie na incydenty związane z danymi.

#### 6. Pomoc Techniczna:

Jak pomóc nie odchodząc od komputera?

Techniki zdalnego wsparcia użytkowników.

Narzędzia do zdalnego zarządzania i rozwiązywania problemów.

Jak zarządzać instalacjami?

Zarządzanie instalacjami oprogramowania z centralnego punktu.

Automatyzacja procesów instalacyjnych.

Ścieżki obsługi zgłoszeń.

Zarządzanie cyklem życia zgłoszeń serwisowych.

Konfiguracja i optymalizacja systemów.

#### 7. Inteligentny Czas:

Porównanie funkcjonalności modułów

Różnice między monitorowaniem aktywności użytkowników a analizą czasu pracy.



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



Zastosowanie modułu w zarządzaniu efektywnością pracy.

Jak czytać dane z modułu?

Interpretacja i analiza danych.

Przykłady raportów i metryk efektywności.

Jak klasyfikować aplikacje?

Kategoryzacja aplikacji według ich użyteczności i wpływu na produktywność.

Narzędzia do automatycznej klasyfikacji aplikacji.

Alarmy i raporty.

Konfiguracja alarmów na podstawie danych.

Tworzenie i zarządzanie raportami efektywności pracy.