

## OPIS PRZEDMIOTU ZAMÓWIENIA DLA:

Pozycja 8 z formularza ofertowego - Oprogramowanie do zarządzania, monitorowania i inwentaryzacji sprzętu IT

Wykonawca zobowiązany jest do dostarczenia oprogramowania spełniającego poniżej wskazane parametry.

### 1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, wdrożenie i uruchomienie kompleksowego systemu zarządzania użytkownikami oraz urządzeniami sieciowymi Zamawiającego. Rozwiązanie ma zapewnić wielowarstwową ochronę, monitorowanie, wykrywanie zmian sprzętowych oprogramowania oraz zagrożeń. Oprogramowanie musi mieć budowę modułową, składającą się z serwera zarządzającego, zdalnych konsoli oraz agentów. Komunikacja pomiędzy serwerem a agentami i konsolami nawiązywana musi być przy użyciu min. szyfrowanego protokołu TLS 1.2.

### 2. Zakres funkcjonalny rozwiązania

System musi spełniać następujące wymagania:

Moduł monitorowania infrastruktury

Moduł musi obejmować serwery oparte na systemach operacyjnych Windows, Linux oraz routery, przełączniki sieciowe w zakresie:

- wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
- wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją OU)
- wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
- wizualizacji urządzeń na mapach z funkcją siatki umożliwiającą korygowanie pozycji ikon na mapie do najbliższej linii siatki
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
- wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze
- wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
- wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny



- zablokowania mapy urzędów przed przypadkową edycją
- serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów
- serwerów pocztowych:
  - program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty
  - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdują się poza zakresem)
  - program ma możliwość wykonywania operacji testowych
  - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa
- monitorowania serwerów WWW i adresów URL
- cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
- obsługi szyfrowania SSL/TLS w powiadomieniach e-mail
- obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID
- obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
- monitoringu routerów i przełączników wg:
  - zmian stanu interfejsów sieciowych
  - ruchu sieciowego
  - podłączonych stacji roboczych – graficzna prezentacja panelu switcha
  - ruchu generowanego przez podłączone do portów stacje robocze
- serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
- Wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
- monitorowania stanu maszyn wirtualnych VMware: działa, nie działa, wstrzymano
- zarządzania stanem maszyn wirtualnych VMware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny
- wydajności systemów Windows:
  - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

## Moduł inwentaryzacji

Moduł musi automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych w zakresie:



- prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
- odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.
- zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
- informacja o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwiające audytowanie i weryfikację użytkowania licencji.
- zbieranie informacji w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej:
- instalacja/deinstalacja aplikacji, zmian adresu IP itd.
- możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiegokolwiek zmiany konfiguracji sprzętowej komputera.
- odczyt numeru seryjnego (klucze licencyjne).
- automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
- przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
- utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
- wymiana plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.
- przechowywanie wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
- przydzielanie dostępu administratorów do zasobów na podstawie praw do oddziałów,
- tworzenie powiązań między zasobami a urządzeniami,
- tworzenie powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
- tworzenie relacji pomiędzy zasobami,
- wskazanie osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
- definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości: dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,



- określenie atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
- masowa edycja atrybutów zasobów,
- definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
- importu danych z zewnętrznego źródła (.CSV),
- Przechowywanie dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
- tworzenie powiązań między zasobami a dokumentami w relacji 1:N,
- oznaczanie statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
- ewidencja czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
- generowanie zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
- przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
- konfiguracja stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
- konfiguracja stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
- archiwizacja i porównywanie audytów zasobów,
- tworzenie kodów kreskowych dla zasobów,
- drukowanie kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
- inwentaryzacja zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
- możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
- inwentaryzacja stacji roboczych niepodłączonych do sieci (bez instalacji Agentów poprzez manualne wykonanie skanów inwentaryzacji offline),
- definiowanie alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnięcie licencji/gwarancja”).
- Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
- informacje o aplikacjach używanych w organizacji.
- tworzenie własnych wzorców aplikacji.
- tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
- informacje o komputerach, na których aplikacja została wykryta.
- zarządzanie posiadanymi licencjami.



- wskazywanie osób odpowiedzialnych za licencję.
- wskazanie użytkowników licencji.
- tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
- rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
- audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
- zarządzanie posiadanymi licencjami: raport zgodności licencji.
- możliwość przypisania do programów numerów seryjnych, wartości itp.

### Moduł obsługi użytkowników

Moduł musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

- faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
- procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
- rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
- informacji o edytowanych przez użytkownika dokumentach,
- historii pracy (cykliczne zrzuty ekranowe),
- listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),
- transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez
- użytkownika),
- wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
- nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Dodatkowo moduł musi posiadać funkcjonalność:

- wykrywania podejrzanej aktywności przez popularne „jigglerzy”, mającej na celu symulowanie faktycznej pracy.





- zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.
- wyszczególnienia podejrzanej aktywności w raportach.
- wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności.
- automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności.
- blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych subdomen (np. \*.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami.
- integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT.
- skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia.
- automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych.
- blokowania ruchu na wskazanych portach TCP/IP,
- blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
- prowadzenia rejestru naruszeń blokad,
- wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,
- przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
- definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.

Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.

#### Moduł zdalnej pomocy użytkownikom

W ramach modułu kontroli stacji użytkownika moduł musi umożliwiać podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połączenie i opcją odrzucenia takiego połączenia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator musi być widoczny ten sam ekran. Funkcja zdalnego dostępu musi również mieć możliwość zasłonięcia ekranu przed użytkownikiem w taki sposób, aby niewidział czynności wykonywanych przez administratora. Administrator w trakcie zdalnego dostępu ma mieć możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy



oraz klawiatury dla użytkownika. Zdalne połączenie musi być również do komputerów, które nie posiadają ekranów (maszyny wirtualne, komputery bez podłączonego monitora lub laptopy z zamkniętym ekranem).

Moduł musi zawierać komunikator (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto czat pozwala na:

- zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej
- rozmowy również między „zwykłymi” użytkownikami
- osadzanie załączników w treści wiadomości,
- osadzanie obrazków w treści wiadomości,
- formatowanie tekstu,
- tworzenie pokoi tematycznych, rozmów grupowych
- oznaczanie kontaktów jako „ulubionych” na liście kontaktów
- uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku
- może być wyświetlany w trybie jasnym lub ciemnym

Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.

Moduł pomocy zdalnej umożliwia również:

- pobieranie listy użytkowników z Active Directory wraz z awatarami,
- wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu,
- adresem e-mail oraz informacją o przełożonym,
- zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
- zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
- zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń,
- zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy,
- tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,



- automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,
- definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,
- przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,
- procesowanie zgłoszeń użytkowników z wiadomości e-mail,
- dostęp do plików źródłowych wiadomości e-mail przetworzonych na zgłoszenia,
- obsługę wielu adresów e-mail jednego użytkownika w celu przetwarzania jako zgłoszeń pochodzących od tej samej osoby,
- eksportowania listy zgłoszeń do plików CSV i XLSX,
- integrację ze wieloma skrzynkami e-mail w celu obsługi różnych kanałów zgłoszeń wraz z automatyzacjami,
- integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,
- tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
- uwzględnianie wyników zgłoszeń na podstawie wyszukiwania informacji z pól niestandardowych,
- współdzielenie pól dodatkowych pomiędzy wieloma kategoriami zgłoszeń,
- dedykowane pola dodatkowe dostępne tylko dla pracowników HelpDesk, administratorów i operatorów,
- informacje zawarte w polach dodatkowych widoczne w kolumnach widoku listy zgłoszeń,
- wykonywanie operacji na wielu zgłoszeniach równocześnie,
- dołączanie załączników do zgłoszeń,
- usuwanie zamkniętych zgłoszeń,
- rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
- szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
- wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
- zrzuty ekranowe (podgląd pulpitu),
- zdalną modyfikację rejestrów,
- dystrybucję oprogramowania przez Agenty,
- definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,
- przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,
- dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
- zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecenia operacji następuje kolejowanie zadania dystrybucji pliku,
- możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,





- możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy,
- planowanie nieobecności pracowników helpdesk,
- obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,
- generowanie raportów obsługi helpdesk,
- zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),
- zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
- wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.

#### Moduł ochrony przed wyciekiem danych

Moduł musi uniemożliwiać wyciek danych z komputerów użytkowników poprzez blokowanie urządzeń. Moduł musi się integrować z Active Directory umożliwiając zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień musi być również do kont użytkowników lokalnych. Moduł musi umożliwiać prowadzenie rejestrów naruszeń i blokad podłączonych nośników.

#### Funkcjonalność modułu:

- blokowanie urządzeń i nośników danych.
- możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera lub uruchomić z nich program zewnętrzny.
- blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
- blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
- blokowanie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
- alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezauważalnych.
- funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
- funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
- funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
- tworzenie list (map) komputerów, które zostały już zaszyfrowane, lub jeszcze nie zostały zaszyfrowane.
- funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.



- funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
- funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.
- funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

#### Zarządzanie prawami dostępu do urządzeń:

- definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
- autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. (urządzenia prywatne są blokowane).
- całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
- centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
- możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

#### Moduł zarządzania czasem i aktywnością użytkowników

Moduł musi dostarczać informacje o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji może oznaczyć sesję aktywności jako czas prywatny gdy wykonuje czynności prywatne na sprzęcie firmowym. Może również uzyskać dostęp do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni mogą uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły pozwalają zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. Dostęp realizowany jest przez przeglądarkę internetową a strona może być wyświetlana w trybie jasnym lub ciemnym.

- statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.
- statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.
- statystyki aktywności podwładnych widoczne dla przełożonego.
- lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem. Wspierane przeglądarki: Microsoft Edge, Mozilla Firefox, Google Chrome, Opera.
- podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.
- statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.



- ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.
- grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.
- możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.
- jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).
- wskaźnik czasu poświęconego na aktywność produktywną.
- definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.
- przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji.
- lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.

Moduł musi posiadać obszar funkcjonalny w postaci platformy WWW który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami, których nazwy można zmieniać wg potrzeb. Na każdym z dashboardów widgety są rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych jest automatycznie odświeżana oraz może być:

- udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem.
- wyświetlana w trybie jasnym lub ciemnym (nocnym).

Dodatkowe wymagania dla oprogramowania.

System musi być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.

Instalator programu musi być zabezpieczony podpisem cyfrowym wystawionym i zweryfikowanym przez zaufany globalny urząd certyfikacji.

Agent musi mieć możliwość wyszukania serwera przez oprogramowanie monitorujące stacje robocze.

Wsparcie techniczne świadczone przez producenta oprogramowania musi być w języku polskim w formie telefonicznej oraz mailowo.