



OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest:

Dostawa przedłużenia ważności licencji oprogramowania do zarządzania infrastrukturą teleinformatyczną dla Urzędu Miasta Ostrów Mazowiecka:

Nazwa	Ilość licencji
Axence nVision Moduły: Network, Inventory, Users, HelpDesk, DataGuard	100

Obecna licencja wygasa 15 marca 2025 r.

Okres odnowienia: od 16 marca 2025 r. do 30 czerwca 2026 r.

2. Przedmiot zamówienia jest współfinansowany ze środków Unii Europejskiej w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu bezpieczeństwa, projekt grantowy „Cyberbezpieczny Samorząd”, tytuł projektu: „Cyberbezpieczny Samorząd – Miasto Ostrów Mazowiecka”.
3. W miejscach, gdzie w opisie wymagań technicznych - równoważnych wskazano znaki towarowe, patenty, pochodzenie, źródło czy szczególny proces, który charakteryzuje produkty dostarczane przez konkretnego Wykonawcę, Zamawiający dopuszcza składanie ofert równoważnych. Za rozwiązanie „równoważne” uznany zostanie zaoferowany produkt, który spełni kryteria/parametry równoważności opisane przez Zamawiającego.
4. Wykonawca, który na etapie składania oferty, powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego rozwiązania spełniają wymagania określone przez Zamawiającego.
5. Instruktaż dla administratorów zamawiającego:
- Wykonawca przeprowadzi instruktaż omawiający wszystkie komponenty, który będzie dotyczył konfiguracji oraz administracji dostarczonego oprogramowania dla administratorów Zamawiającego.
 - Wykonawca zapewni uczestnikom odpowiednie materiały szkoleniowe w formie elektronicznej.
 - Program Instruktażu powinien obejmować zagadnienia związane z czynnościami instalacyjnymi, konfiguracyjnymi i administracyjnymi wdrażanego systemu.
 - Instruktaż musi być przeprowadzony w języku polskim.
 - W instruktażu będzie uczestniczyć 2 osoby.
6. Minimalne parametry techniczno-jakościowe Przedmiotu zamówienia przedstawione zostały poniżej:

LICENCJA	W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji w okresie ważności licencji. W ramach licencji Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do serwisu producenta.
-----------------	---

	Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie elektronicznej lub papierowej. Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.
Monitorowanie infrastruktury bezagentowo	obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie: • wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping • wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o 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 urządzeń 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 znajdą 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 Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program posiada również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP. Program umożliwia również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitu, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy pozwalają na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie umożliwia wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0 Program ma możliwość integracji ze sprzętową bramką GSM HW-SMS-GW 3 w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP) oraz poprzez integrację z bramkami SMSEagle.
Inwentaryzacja sprzętu i oprogramowania	program automatycznie gromadzi informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz: 1. Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp. 2. Umożliwia odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe. 3. Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 4. Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. 5. Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. 6. Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku

	zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. 7. Umożliwia odczytanie numeru seryjnego (klucze licencyjne). 8. Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. 9. Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. 10. Umożliwia 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). 11. Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane. Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania: • przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, • przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów, • tworzenia powiązań między zasobami a urządzeniami, • tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych, • tworzenia relacji pomiędzy zasobami, • wskazania 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, • określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, • masową edycję atrybutów zasobów, • definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, • importu danych z zewnętrznego źródła (.CSV), • przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., • tworzenia powiązań między zasobami a dokumentami w relacji 1:N, • oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., • ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, • generowania 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, • konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, • konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, • archiwizacji i porównywania audytów zasobów, • tworzenia kodów kreskowych dla zasobów, • drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, • inwentaryzacji 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, • inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), • definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnięcie licencja/gwarancja”). • Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez: 1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. 2. Informacje o aplikacjach używanych w organizacji. 3. Tworzenie własnych wzorców aplikacji. 4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. 5. Informacje o komputerach, na których aplikacja została wykryta. 6. Zarządzanie posiadanymi licencjami. 7. Wskazywanie osób odpowiedzialnych za licencję. 8. Wskazanie użytkowników licencji. 9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. 10. 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. 11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych. 12. Zarządzanie posiadanymi licencjami: raport zgodności licencji. 13. Możliwość przypisania do programów numerów seryjnych, wartości itp. Okna audytowe posiadają możliwość filtrowania elementów per oddział.
Obsługa użytkowników	program umożliwia 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 użytkownika 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. Program ponadto posiada możliwość: • 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 sub-domen (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 domen; 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. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane
--	---

	między grupami lub kontami. Program posiada Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.
Zdalna pomoc użytkownikom	W ramach kontroli stacji użytkownika dostępny jest 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 widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu umożliwia równoczesne podłączenie do tego samego komputera kilku administratorom. W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie pozwala na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł umożliwia również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Kolejną ważną funkcjonalnością jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. System umożliwia użycie pośredniego statusu „zgłoszenie rozwiązane” przed ostatecznym zamknięciem zgłoszenia. Moduł ten zawiera również 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 W module zawarta jest również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program umożliwia informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Użytkownik ma możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z

	poziomu ikony Agenta. Administrator ma możliwość tworzenia szkiców i archiwizowania komunikatów. Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany jest przez dedykowany portal dostępny przez przeglądarkę internetową, który 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, • 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 kolejkowanie 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.
Ochrona danych przed wyciekiem	1. Blokowanie urządzeń i nośników danych. Program ma możliwość zarządzania prawami 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. 2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskiectek. 3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. 4. Blokowanie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane. 5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezauważanych. 6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender. 7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker. 8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker. 9. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu. 10. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu. 11. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender. 12. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM. Zarządzanie prawami dostępu do urządzeń: 1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. 2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.

	3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. 4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. 5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane. Audyt operacji na plikach na urządzeniach przenośnych: 1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. 2. Podłączenie/odłączenie urządzenia przenośnego. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. Definiowanie reguł monitorowanych folderów w postaci list. Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.) Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych. Program umożliwia prowadzenie rejestru naruszeń blokad podłączanych nośników.
Portal informacyjny WWW	Oprogramowanie posiada również obszar funkcjonalny w formie 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). Oprogramowanie umożliwia zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego. Widgety prezentują dane ze wszystkich modułów funkcjonalnych oprogramowania: • Mapa sieci, • Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci, • Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów, • Statystyki z obszaru wydruków, Statystyki użycia aplikacji, Użycie łącza, Aktywność WWW, naruszenia reguł blokad, • Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie, • Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem), informacje o stanie Bitlocker, Windows Defender, Windows Firewall, naruszenia reguł dostępu do nośników danych, • Produktywność dla grupy, Statystyki czasu nieproduktywnego.
Inne	Ochrona przed usunięciem Program jest zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje. Funkcjonalność Agenta Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.

	Zabezpieczenia Instalator programu jest zabezpieczony podpisem cyfrowym wystawionym i zweryfikowanym przez zaufany globalny urząd certyfikacji (CA). Wyszukiwarka Globalna wyszukiwarka, zwracająca wyniki obiektów różnego typu na podstawie wyszukiwanych słów kluczowych, np.: urządzenia, użytkownicy, zasoby, elementy interfejsu konsoli zarządzającej, elementy opcji. Wsparcie techniczne Wsparcie techniczne świadczone jest telefonicznie lub mailowo w języku polskim.
--	--