







FUNKCJE WSPÓLNE NVISION		NETWORK	INVENTORY	USERS	HELPDESK	DATAGUARD	SMARTTIME
OGÓLNE	ADMINCENTER						
<ul style="list-style-type: none"> Agent na Windows ochrona Agenta przed usunięciem pakiet narzędzi diagnostycznych Axence netTools alarmy zdarzenie-akcja powiadomienia (pulpitowe, e-mailowe, SMS-owe) oraz akcje korekcyjne (uruchomienie programu, restart komputera itp.) powiadomienie o alarmach wysyłane za pośrednictwem komunikatorów MS Teams i Slack wysyłka powiadomień o alarmach za pośrednictwem serwisu smsapi.pl obsługa OAuth 2.0 dla wysyłki wiadomości e-mail i SMS zarządzanie hierarchią użytkowników (w tym import z AD) raporty dla użytkowników, urządzeń, oddziałów, map sieci lub całego atlasu jednoczesna praca wielu administratorów, dziennik dostępu administratorów zarządzanie uprawnieniami wielu administratorów zarządzanie grupami (tworzenie, przypisywanie użytkowników) 	<ul style="list-style-type: none"> prezentowanie wybranych danych z nVision w przeglądarce internetowej za pomocą widgetów responsywne widgety, zarządzanie rozmiarem siatki widgetów automatyczne odświeżanie dashboardów wyświetlanie dashboardów w trybie jasnym i ciemnym udostępnianie dashboardów w trybie tylko do odczytu zarządzanie uprawnieniami administratorów do funkcjonalności AdminCenter widgety dla modułu Network: liczniki wydajności, alarmy oraz odpowiedzi serwisów TCP/IP, mapa sieci widgety dla modułu Inventory: zmiany w konfiguracji sprzętowej urządzeń z Agentami, zmiany w liście zainstalowanego oprogramowania, alarmy dla zasobów 	<ul style="list-style-type: none"> skanowanie sieci, wykrywanie urządzeń i serwisów TCP/IP interaktywne mapy sieci, mapy użytkownika, oddziałów, mapy inteligentne serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.) liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp. działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń liczniki SNMP v1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne) 	<ul style="list-style-type: none"> IT Asset Management – zarządzanie wszelkimi zasobami, za które odpowiada dział IT szczegółowe informacje i ewidencja czynności wykonywanych na zasobach w trakcie całego cyklu życia, możliwość definiowania statusów i pól oraz generowanie protokołu przekazania sprzętu widok zasobów, aplikacji, dokumentów, licencji dla poszczególnych użytkowników lub osobny widok według zasobów przypisanych do urządzeń jednoczesne przypisywanie dokumentu do wielu zasobów uprawnienia dostępu administratorów do typów zasobów, licencji i dokumentów w ramach oddziałów masowa edycja atrybutów zasobów, np. statusu. Software Asset Management – rozbudowany system zarządzania aplikacjami i licencjami, identyfikacja realnego zużycia licencji rozliczanie dowolnego typu licencji, w tym modelowanie licencji chmurowych rozliczanie licencji według użytkownika, urządzenia, numeru seryjnego lub na podstawie wersji zainstalowanej aplikacji audyt inwentaryzacji sprzętu i oprogramowania wgląd w licencje przypisane do użytkownika pracującego na wielu urządzeniach zdalny dostęp do menadżera plików z możliwością usuwania plików użytkownika 	<ul style="list-style-type: none"> pełne zarządzanie użytkownikami, bazujące na grupach i politykach bezpieczeństwa blokowanie uruchamianych aplikacji monitorowanie wiadomości e-mail (nagłówki) – antyphishing szczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy) użytkowane aplikacje (aktywnie i nieaktywnie) odwiedzane strony WWW (tytuły i adresy stron, liczba i czas wizyt) audyty wydruków (drukarka, użytkownik, komputer), koszty wydruków statyczny zdalny podgląd pulpitu użytkownika (bez dostępu) zrzuty ekranowe (historia pracy użytkownika ekran po ekranie) blokowanie stron WWW rejestr naruszeń blokad agregujący informacje o próbie dostępu do blokowanych stron WWW, uruchamianiu zakazanych aplikacji oraz pobieraniu plików z niedozwolonymi rozszerzeniami 	<ul style="list-style-type: none"> tworzenie i procesowanie zgłoszeń serwisowych poprzez intuicyjny interfejs webowy lub za pośrednictwem maila planowanie zastępstw w przydzielaniu zgłoszeń możliwość wskazania osób, które muszą zaakceptować zgłoszenie tworzenie ścieżek akceptacji na podstawie kategorii automatyczna wysyłka powiadomień do osób akceptujących zgłoszenie kiosk z aplikacjami – możliwość stworzenia listy bezpiecznych aplikacji do samodzielnej instalacji przez użytkownika obsługa umów o gwarantowanym poziomie świadczenia usług (SLA) automatyczne przypisywanie zgłoszeń do obsługującego na podstawie określonych warunków zarządzanie kategoriami i priorytetami zgłoszeń oraz powiadomieniami z HelpDesku wyszukiwarka oraz aktualizacja zgłoszeń w czasie rzeczywistym definiowanie reguł widoczności zgłoszeń oraz automatyzacje bazujące na warunkach ograniczenie tworzenia zgłoszeń i dostępności artykułów w bazie wiedzy przez wybrane grupy użytkowników tylko w określonych kategoriach rozbudowany system raportów przetwarzanie zgłoszeń w trybie anonimowym komentarze i załączniki w zgłoszeniach; dodawanie pól niestandardowych wizytówki użytkowników 	<ul style="list-style-type: none"> informacje o urządzeniach podłączonych do danego komputera lista wszystkich urządzeń podłączonych do komputerów w sieci audyt (historia) połączeń i operacji na urządzeniach przenośnych oraz udziałach sieciowych i dyskach lokalnych monitorowanie operacji na plikach w katalogach na dysku systemowym monitorowanie operacji na plikach z zasobów sieciowych udostępnianych przez urządzenia nieobsługiwane przez Agentą np. macierze Synology, Qnap itp. zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników centralna konfiguracja: ustawienie reguł dla całej sieci oraz grup i użytkowników Active Directory integracja bazy użytkowników i grup z Active Directory alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym oraz na dyskach lokalnych 	<ul style="list-style-type: none"> statystyki czasu pracy: godzina rozpoczęcia i zakończenia aktywności, czas przy komputerze, czas poza komputerem szczegółowe statystyki czasu pracy przy komputerze oraz historia pracy w widoku graficznym: lista aplikacji desktopowych i odwiedzanych stron WWW statystyki aktywności osobistej widoczne dla pracownika statystyki aktywności grupy i jej członków widoczne dla menedżera grupy statystyki aktywności podwładnych widoczne dla przełożonego podgląd zrzutu ekranu użytkownika dla menedżerów i administratorów kategoryzowanie aplikacji i stron WWW (np. aplikacje biurowe, komunikatory, rozrywka): predefiniowana lista kategorii z możliwością edycji dodawanie wyjątków przez administratora grupy, wskazujących, że dana aplikacja w tej grupie jest uznawana za produktywną

FUNKCJE WSPÓLNE NVISION		 NETWORK	 INVENTORY	 USERS	 HELPDESK	 DATAGUARD	 SMARTTIME
OGÓLNE	ADMINCENTER						
<ul style="list-style-type: none"> • menu kontekstowe z możliwością definiowania własnych narzędzi • dziennik dostępu administratorów: wysyłanie zdarzeń do zewnętrznego kolektora Syslog • globalna wyszukiwarka w konsoli nVision; globalne wyszukiwanie obiektów np.: urządzeń, użytkowników, zasobów oraz elementów interfejsu programu (np. opcji) • logowanie w konsoli deinstalacji Agenta • obsługa OAuth 2.0 dla wysyłki wiadomości e-mail i SMS • uwierzytelnianie wieloskładnikowe (Multifactor Authentication/MFA) • zwiększone wymagania dla haseł użytkowników • szyfrowana synchronizacja z Active Directory z wykorzystaniem LDAPS (Secure LDAP) 	<ul style="list-style-type: none"> • widżety dla modułu Users: statystyki z obszaru wydruków, statystyki użycia aplikacji, użycie łącza, aktywność WWW, rejestr naruszeń blokad • widżety dla modułu HelpDesk: statystyki z obsługi zgłoszeń, lista najnowszych nierozwiązanych zgłoszeń, lista najstarszych nierozwiązanych zgłoszeń, ostatnie 10 zgłoszeń ze złamaną metryką SLA, 10 najbliższych metryk SLA • widżety dla modułu DataGuard: ostatnio podłączone nośniki zewnętrzne, ostatnie operacje na plikach, BitLocker, antywirus, firewall • widżety dla modułu SmartTime: produktywność dla grupy, statystyki czasu nieproduktywnego 	<ul style="list-style-type: none"> • kompilator plików MIB • obsługa pułapek SNMP • routery i switche: mapowanie portów; informacja, do którego przełącznika jest podłączone urządzenie • obsługa komunikatów Syslog • obsługa szyfrowania AES, DES i 3DES dla protokołu SNMPv3 • możliwość nakładania na urządzenie liczników wydajności wg szablonu (wzorca) • monitorowanie i zarządzanie maszynami wirtualnymi VMware 	<ul style="list-style-type: none"> • informacje o wpisach rejestrowych, plikach i archiwach .zip na stacji roboczej • szczegółowe informacje o konfiguracji sprzętowej konkretnej stacji roboczej • zarządzanie instalacjami/deinstalacjami oprogramowania przez menedżera pakietów MSI • alarmy: instalacja oprogramowania, zmiana w zasobach sprzętowych • aplikacja dla systemu Android umożliwiająca spis z natury na bazie kodów kreskowych, kodów QR, generowanie etykiet w konsoli nVision • możliwość archiwizacji i porównywania audytów • mobilny Asystent Inwentaryzacji dla systemu Android: wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycja zasobów, dodawanie czynności serwisowych, drukowanie etykiet • generator dokumentów na podstawie szablonów • automatyczne numerowanie dodawanych zasobów oraz dokumentów wg zdefiniowanego wzorca numeracji • historia użycia konkretnej licencji oprogramowania • odczyt danych S.M.A.R.T. z dysków NVMe 	<ul style="list-style-type: none"> • dedykowane alarmy dla wszystkich rodzajów incydentów zbieranych przez rejestr naruszeń blokad • możliwość korzystania z zewnętrznych list blokowania stron, w tym z listą ostrzeżeń CERT.PL • zgodność z RODO – przyporządkowanie konfiguracji, uprawnień i dostępu do konkretnego użytkownika niezależnie od urządzenia • informatyka śledcza – szczegółowe wyszczególnienie aktywności oraz metryki użytkownika • blokowanie uruchamiania procesów na podstawie lokalizacji pliku .EXE • reguły filtrowania stron WWW i blokowania aplikacji: zmiana mechanizmu tworzenia i zarządzania regułami, grupowanie reguł • reguły filtrowania stron WWW i blokowania aplikacji: powielanie reguł między grupami użytkowników • możliwość wykrywania podejrzanych aktywności użytkowników za pomocą mechanizmu wykrywajęcemu jigglery • możliwość użycia maski * w wykluczeniach w integracji ze stosem TCP/IP 	<ul style="list-style-type: none"> • wewnętrzny komunikator (czat) z możliwością przesyłania plików • jednoczesna praca wielu administratorów z komunikatami • komunikaty do użytkowników/komputerów z opcją obowiązkowego potwierdzenia odczytu • wyświetlanie historii komunikatów w Agencji • szkice i archiwizacja komunikatów • zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury • równoczesny zdalny dostęp kilku administratorów do jednego Agent; pełna obsługa sesji terminalowych • możliwość wyboru wyświetlanego ekranu w trakcie trwania zdalnego dostępu • integracja użytkowników z Active Directory • zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania); dwukierunkowa wymiana plików • baza wiedzy z wbudowaną wyszukiwarką i możliwością dodawania multimediów • zdalny dostęp do menedżera plików z możliwością usuwania plików użytkownika • zarządzanie kontami lokalnych użytkowników Windows • dokumenty prawne dot. ochrony sygnalistów • możliwość dodania opisu kategorii zgłoszenia np. w celu umieszczenia klauzuli RODO • dark mode w systemie zgłoszeń i w czacie • zdalna edycja rejestru na komputerach z zainstalowanym Agentem nVision • możliwość eksportu listy zgłoszeń do pliku 	<ul style="list-style-type: none"> • atrybut „nośnik zaufany” • automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa • możliwość usuwania nieistniejących/zutilizowanych nośników danych (np. USB) • metryki użytkowników prezentujące aktualne ustawienia dla danego pracownika • integracja z Windows Defender: zarządzanie ustawieniami wbudowanego antywirusa wraz z możliwością alarmowania o wykrytych problemach oraz wynikach skanowania • wykrywanie oprogramowania antywirusowego innego niż Windows Defender • integracja z Windows BitLocker: odczyt stanu modułu TPM oraz zaszyfrowania woluminów • możliwość zdalnego szyfrowania dysków za pomocą funkcji BitLocker • integracja z Windows Firewall: włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych 	<ul style="list-style-type: none"> • klasyfikacja produktywności aplikacji desktopowych i stron WWW: produktywność, neutralność, nieproduktywność – z możliwością przypisania wyjątku produktywności dla wybranej grupy pracowników • metryki produktywności: czas poświęcony na aktywność produktywną, produktywność wyliczana procentowo na podstawie statystyk czasu pracy • definiowanie wymaganego w organizacji progu produktywności i limitu nieproduktywności – z możliwością włączenia alarmów e-mailowych dla menedżerów • lista kontaktów w organizacji • czas prywatny – możliwość wyłączenia analizy aktywności w SmartTime w czasie używania służbowego komputera do celów prywatnych • dark mode w aplikacji produktywności • odseparowanie wskaźników produktywności podgrup należących do głównej grupy podległej wybranemu menedżerowi • możliwość ograniczenia dostępnych kontaktów