

OR-3.271.1.2024

Załącznik nr 1 do zapytania ofertowego

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu IT oraz oprogramowania w ramach realizacji projektu grantowego „Cyberbezpieczny Samorząd”

I. Wstęp

Niniejszy dokument stanowi szczegółowy opis przedmiotu zamówienia na zakup sprzętu wraz z oprogramowaniem.

II. Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. Sprzedaż i dostarczenie fabrycznie nowego Sprzętu i Oprogramowania;
2. udzielenie przez Wykonawcę gwarancji i zapewnienie w jej ramach serwisu gwarancyjnego i wsparcia technicznego na dostarczony Sprzęt;
3. udzielenie licencji na Oprogramowanie;
4. dostarczenie przez Wykonawcę Dokumentacji dostarczonego Sprzętu.

III. Wymagania ogólne dot. zamówienia

Numer wymagań	Opis wymagania
O.1	W przypadkach, kiedy w szczegółowym opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.
O.2	W sytuacjach, kiedy Zamawiający opisuje szczegółowy przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 30 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne opisane, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.
O.3	Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w SOPZ.

	Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.
O.4	Dla jednoznacznej identyfikacji oferowanego sprzętu należy podać co najmniej nazwę producenta, a także nazwę i model oferowanego sprzętu. Zamawiający wymaga również podania faktycznych parametrów sprzętu, o którym mowa w pkt O.5 poniżej, w taki sposób, by oceniający byli w stanie stwierdzić, czy zaoferowany sprzęt spełnia wymagania specyfikacji. Przedmiotowe informacje są składane na potwierdzenie, iż oferowane urządzenia spełniają wymagania Zamawiającego.
O.5	<p>O ile inaczej nie zaznaczono, wszelkie zapisy SOPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne, np. zapis:</p> <p>„Procesor klasy x64, 2 rdzeniowy, 4 wątkowy, niskonapięciowy o TDP 15W, zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem co najmniej 2,40 GHz, z możliwością taktowania 3,8 GHz, z pamięcią last level cache CPU co najmniej 4 MB lub równoważny 2 rdzeniowy 4 wątkowy procesor klasy x86 Zaoferowany procesor musi uzyskiwać jednocześnie w teście Passmark CPU Mark wynik min.: 6000 punktów</p> <p>należy rozumieć jako:</p> <p>„Procesor klasy x64, co najmniej 2 rdzeniowy, co najmniej 4 wątkowy, niskonapięciowy o TDP 15W, zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem co najmniej 2,40 GHz, z możliwością taktowania co najmniej 3,8 GHz, z pamięcią last level cache CPU co najmniej 4 MB lub równoważny, co najmniej 2 rdzeniowy co najmniej 4 wątkowy procesor klasy x64 Zaoferowany procesor musi uzyskiwać jednocześnie w teście Passmark CPU Mark wynik co najmniej 6000 punktów.</p>
O.6	Dostarczany sprzęt musi być fabrycznie nowy i wyprodukowany nie wcześniej niż w czerwcu 2024 r.
O.7	Dostarczany sprzęt musi mieć okablowanie, zasilacze oraz wszystkie inne komponenty, zapewniające właściwą instalację i użytkowanie (np. przewody zasilające itp).
O.8	Sprzęt musi być dostarczony ze wszystkimi niezbędnymi do działania i zapewnienia wymaganych funkcjonalności bezterminowymi licencjami na używanie tych funkcjonalności.
O.9	Dokumenty gwarancyjne wystawiane lub przekazywane przez Wykonawcę powinny być zgodne z SIWZ oraz z zapisami zawartymi w § 6 Wzoru umowy w sprawie zamówienia publicznego na Dostawa sprzętu IT oraz oprogramowania w ramach realizacji projektu grantowego „Cyberbezpieczny Samorząd”.

IV. Wymagania szczegółowe Zamawiającego:

ZAKUPU SPRZĘTU IT DLA URZĘDU GMINY KOŚCIELEC

1. ZAPORA SIECIOWA TYPU UTM – 1 sztuka

Zakup sprzętu w ramach programu Trade-Up, posiadanego urządzenia FortiGate 40F o numerze seryjnym: FGT40FTK20031678 wraz z elektroniczną licencją na 10 Tokenów Software'owych

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	<p>System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"> 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	<ol style="list-style-type: none"> 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: <ul style="list-style-type: none"> • 8 portami Gigabit Ethernet RJ-45. • 2 gniazdami SFP+ 10 Gbps. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe	<ol style="list-style-type: none"> 1. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B.

	<ol style="list-style-type: none"> Przepustowość Stateful Firewall: nie mniej niż 27 Gbps dla pakietów 64 B. Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 25 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 4 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2 Gbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.5 Gbps.
Funkcje Systemu Bezpieczeństwa	<p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none"> Kontrola dostępu - zaporą ogniową klasy Stateful Inspection. Kontrola Aplikacji. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. Ochrona przed malware. Ochrona przed atakami - Intrusion Prevention System. Kontrola stron WWW. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. Zarządzanie pasmem (QoS, Traffic shaping). Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wystanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	<ol style="list-style-type: none"> Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: <ul style="list-style-type: none"> Translację jeden do jeden oraz jeden do wielu. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

	<p>7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.</p> <ul style="list-style-type: none"> • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • Nuage Networks VSP. • OpenStack. • VMware vCenter (ESXi). • VMware NSX. • VMware NSX.Nutanix. • VMware NSX.IBM Cloud. • Kubernetes.
Połączenia VPN	<p>1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługę protokołu Diffie-Hellman grup 19, 20 oraz 21. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Dynamiczne zestawianie tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. <p>2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączny WAN	<p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <ol style="list-style-type: none"> 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).

	<ol style="list-style-type: none"> 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv6), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	<ol style="list-style-type: none"> 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). 3. Reguły SD-WAN umożliwiają określenie aplikacji jako argumentu dla kierowania ruchu. 4. Rozwiązanie powinno wspierać funkcję Forward Error Correction na tunelach IPSec. 5. Funkcja monitorowania łączy w oparciu o rzeczywisty ruch bez konieczności tworzenia dedykowanych detektorów.
Zarządzanie pasmem	<ol style="list-style-type: none"> 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	<ol style="list-style-type: none"> 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami	<ol style="list-style-type: none"> 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	<ol style="list-style-type: none"> 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 21). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	<ol style="list-style-type: none"> 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość

	<p>określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.</p> <ol style="list-style-type: none"> Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. Filtrowanie treści wideo w oparciu o kategorie - co najmniej dla serwisów: youtube, vimeo. Blokowanie wysyłania poświadczeń firmowych do obcych serwisów.
Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none"> System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: <ul style="list-style-type: none"> Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	<ol style="list-style-type: none"> Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	<ol style="list-style-type: none"> Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu,

	<p>aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p> <ol style="list-style-type: none"> Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. Możliwość włączenia logowania per reguła w polityce firewall. System zapewnia możliwość logowania do serwera SYSLOG. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	<p>Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:</p> <ul style="list-style-type: none"> Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.
Gwarancja oraz wsparcie	System jest objęty serwisem gwarancyjnym producenta przez okres min. 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

2. PRZEŁĄCZNIK SIECIOWY – 3 sztuki

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	<p>W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.</p> <p>W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymagany jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa.</p>
Parametry fizyczne platformy	<ol style="list-style-type: none"> 1. Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. 2. Zasilanie AC 230V. 3. Budżet mocy dla portów PoE min.: 370 W. 4. Maksymalny pobór mocy bez budżetu dla PoE: 110 W. 5. Minimalny zakres temperatury pracy: 0-40°C.
Interfejsy sieciowe	<ol style="list-style-type: none"> 1. Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: <ul style="list-style-type: none"> • 48 porty GE RJ-45. W tym porty PoE w ilości co najmniej: 24, zgodne ze standardem: 802.3af oraz 802.3at. • 4 porty 10 GE SFP+.
Zarządzanie	<ol style="list-style-type: none"> 1. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). 2. Wsparcie dla SNMP w wersjach 1-3 3. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. 4. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. 5. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. 6. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). 7. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. 8. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. 9. Automatycznie wykonywane rewizje konfiguracji.
Parametry wydajnościowe	<ol style="list-style-type: none"> 1. Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. 2. Tablica adresów MAC o pojemności co najmniej 32k wpisów. 3. Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
Wymagane funkcje	<ol style="list-style-type: none"> 1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. 2. Obsługa Jumbo Frames.

	<ol style="list-style-type: none"> Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). Agregacja portów zgodna ze standardem 802.3ad. Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. Obsługa routingu statycznego. Port-mirroring. Uwierzytelnianie 802.1x na poziomie portu. Uwierzytelnianie 802.1x w oparciu o adres MAC. W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. Obsługa protokołu sFlow.
Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	<ol style="list-style-type: none"> Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: <ul style="list-style-type: none"> Centralne zarządzanie konfiguracją urządzenia Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania Centralne zarządzanie sieciami VLAN. Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. Automatyczna detekcja i rekomendacje konfiguracji. Przesyłanie logów na zewnętrzny serwer syslog. Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. Obsługa białych i czarnych list adresów MAC. Wykrywanie aplikacji komunikujących się w sieci. Musi być możliwe redundantne połączenie z elementami zarządzającymi. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	<ol style="list-style-type: none"> System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
Gwarancja oraz wsparcie	<ol style="list-style-type: none"> System musi być objęty serwisem gwarancyjnym producenta przez okres min. 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

3. ACCESS POINT, sztuk 4

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.
Parametry fizyczne	<ol style="list-style-type: none"> Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych: <ul style="list-style-type: none"> Temperatura 0–50°C, Wilgotność 5–90%. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy: <ul style="list-style-type: none"> 2.4 GHz 802.11b/g/n, 5 GHz 802.11a/n/ac/ax, Skaner 2.4GHz i 5GHz
Parametry wydajnościowe	<ol style="list-style-type: none"> Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID. Urządzenie musi być wyposażone w moduł BLE. Urządzenie musi być wyposażone w dwa interfejsy Ethernet 10/100/1000 Base-TX, Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych: <ul style="list-style-type: none"> Tunnel, Bridge, Mesh. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.11i, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA). Interfejs radiowy urządzenia powinien wspierać następujące funkcje: <ul style="list-style-type: none"> MIMO – 2x2, Maksymalna przepustowość dla poszczególnych modułów radiowych: <ul style="list-style-type: none"> 574 Mbps; 1201 Mbps; Wymagana moc nadawania: <ul style="list-style-type: none"> min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm; min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm; Wsparcie dla 802.11n 20/40MHz HT, Wsparcie dla kanałów 80MHz, Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy, Maksymalna deklarowana liczba klientów per moduł radiowy: <ul style="list-style-type: none"> 512; 512; Funkcje dodatkowe:

	<ul style="list-style-type: none"> • OFDMA UL i DL • Spatial Reuse (B • DL-MU-MIMO • SS Coloring) • UL-MU-MIMO 802.11ax • DL-MU-MIMO • Enhanced Target Wake Time (TWT)
Gwarancja oraz wsparcie	<p>Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.</p>

4. OPROGRAMOWANIE ANTYWIRUSOWE TYPU EDR, 45 LICENCJI

Parametr	Charakterystyka (wymagania minimalne)
Administracja zdalna w chmurze	<ol style="list-style-type: none"> Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
Ochrona stacji roboczych	<ol style="list-style-type: none"> Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). Rozwiązanie musi wspierać architekturę ARM64. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.

9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
 - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
 - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

	<ol style="list-style-type: none"> 22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. 23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: <ul style="list-style-type: none"> • tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, • tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. 24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. 25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. 29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty
Ochrona serwera	<ol style="list-style-type: none"> 1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. 9. Dodatkowe wymagania dla ochrony serwerów Windows: 10. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 11. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na goście (HIPS). 12. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.

	<ol style="list-style-type: none"> 13. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 14. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 15. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 16. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 17. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 18. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. 19. Dodatkowe wymagania dla ochrony serwerów Linux: 20. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 21. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 22. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 23. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszzonego mikro-serwisu.
Szyfrowanie	<ol style="list-style-type: none"> 1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit. 2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 3. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
Ochrona urządzeń mobilnych opartych o system Android	<ol style="list-style-type: none"> 1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: <ul style="list-style-type: none"> • usunięcie zawartości urządzenia, • przywrócenie urządzenie do ustawień fabrycznych, • zablokowania urządzenia, • uruchomienie sygnału dźwiękowego, • lokalizację GPS.

	<ol style="list-style-type: none"> 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: <ul style="list-style-type: none"> • nazwę aplikacji, • nazwę pakietu, • kategorię sklepu Google Play, • uprawnienia aplikacji, • pochodzenie aplikacji z nieznanego źródła.
Sandbox w chmurze	<ol style="list-style-type: none"> 1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 2. Rozwiązanie musi wykorzystywać do działania chmurę producenta. 3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. 6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 7. Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów. 8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. 9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. 11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzewać jakie pliki zostały wysłane do analizy oraz przez kogo. 12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: <ul style="list-style-type: none"> • Czysty, • Podejrzany, • Bardzo podejrzany, • Szkodliwy. 13. przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. 14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. 15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.
Moduł XDR	<ol style="list-style-type: none"> 1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.4. 4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
16. Konsola administracyjna musi mieć możliwość tagowania obiektów.
17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell..

5. DYSKI TWARDE, sztuk 4

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	Dyski twarde przeznaczone do serwera NAS kompatybilna z istniejącą jednostką Synology RS818+
Rozmiar	3,5"
Wielkość Cache	256 MB
MTBF	2 500 000 h
Ilość obrotów	7200 RPM
Typ Interfejsu	SATA 6Gb kompatybilny z 3.0
Wielkość RAW dysku	14 TB
Długość gwarancji	60 miesięcy
Maksymalny transfer w MB/s	260
Sposób chłodzenia	Hel
Wbudowany czujnik drgań	Tak

6. OPROGRAMOWANIE/PLATFORMA TYPU SIEM, sztuk 1

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	<p>W ramach postępowania wymagany jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.</p> <p>Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi wersje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).</p>
Interfejsy, Dysk:	System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB
Parametry wydajnościowe	<ol style="list-style-type: none"> System musi być w stanie przyjmować minimum 5 GB logów na dzień. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.
W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:	
Logowanie	<ol style="list-style-type: none"> Podgląd logowanych zdarzeń w czasie rzeczywistym. Możliwość przeglądania logów historycznych z funkcją filtrowania. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: <ul style="list-style-type: none"> Listę najczęściej wykrywanych ataków. Listę najbardziej aktywnych użytkowników. Listę najczęściej wykorzystywanych aplikacji. Listę najczęściej odwiedzanych stron www. Listę krajów, do których nawiązywane są połączenia. Listę najczęściej wykorzystywanych polityk Firewall. Informacje o realizowanych połączeniach IPSec. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
Raportowanie	<p>W zakresie raportowania system musi zapewniać:</p> <ol style="list-style-type: none"> Generowanie raportów co najmniej w formatach: PDF, CSV. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. Funkcję definiowania własnych raportów.

	<ol style="list-style-type: none"> Możliwość spolszczenia raportów. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.
Korelacja logów	<p>W zakresie korelacji zdarzeń system musi zapewniać:</p> <ol style="list-style-type: none"> Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: <ul style="list-style-type: none"> Malware. Aplikacje sieciowe. Email. IPS. Traffic. Systemowe: utracone połączenie vpn, utracone połączenie sieciowe. Funkcję zarządzania zdarzeniami z automatyzacją zadań, która może być konfigurowalna za pomocą playbooków składających się z reakcji i sekwencji zautomatyzowanych działań.
Zarządzanie	<ol style="list-style-type: none"> System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. <ul style="list-style-type: none"> Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
Serwisy i licencje	<ol style="list-style-type: none"> System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. Wsparcie: System musi być objęty serwisem producenta przez okres 24 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
Opisy do wymagań ogólnych	<ol style="list-style-type: none"> Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora

producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

7. SYSTEMU DO ZARZĄDZANIA INFRASTRUKTURĄ IT I ZASOBAMI LUDZKIMI, 50 klientów

Parametr	Charakterystyka (wymagania minimalne)
Zarządzanie zasobami	
Pozyskiwanie informacji o sprzęcie, zarządzanie widokami, funkcje ogólne	<ol style="list-style-type: none"> 1. Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania 2. Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP oraz SNMP 3. Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o aktualizacji 4. Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy 5. Odzworowanie struktury organizacji w oparciu o Active Directory 6. Jednostronna synchronizacja komputerów oraz drukarek z AD oraz AAD (Odzworowanie wszystkich wprowadzonych zmian w rekordach Active Directory) 7. Automatyczne skanowanie całości lub wybranych grup Active Directory (oraz AAD) oraz sieci 8. Mapowanie atrybutów obiektów AD (oraz AAD) do obiektów w programie 9. Grupowanie wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów, lokalizacji, statusów) 10. Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.) 11. Utworzenie własnych typów elementów wyposażenia 12. Łączenie elementów wyposażenia w zestawy 13. Przypisywanie zasobu do wielu zestawów 14. Makrodefinicje w celu spersonalizowania nazw elementów w drzewku wyposażenia 15. Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach 16. Podpięcie dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików 17. Przypisywanie sprzętu do konkretnych osób 18. Przypisywanie sprzętu do wybranej firmy 19. Automatyczne wyznaczanie 'Głównego użytkownika' komputera 20. Wiązanie wielu rekordów wyposażenia z użytkownikiem 21. Przypisywanie sprzętu do dowolnej lokalizacji 22. Definiowanie własnych, dowolnych atrybutów sprzętu 23. Aktywnym komputerom (bez określonego statusu) przydzielany jest status 'W użyciu' 24. Wydruk etykiet z kodami kreskowymi do inwentaryzacji wyposażenia 25. Dowolna treść kodu kreskowego 26. Określanie loga firmy oraz użycia go na wydrukach 27. Grupowa zmiana domeny/grupy roboczej zasobu
Informacje o sprzęcie	<ol style="list-style-type: none"> 1. Automatyczne wykrywanie typu komputera (Desktop\Notebook\Serwer\Kontroler domeny) na podstawie wyników skanowania sprzętu 2. Wykrywanie komputerów typu All-In-One 3. Automatyczne wykrywanie typów stacji roboczej (Tower\Desktop\SFF\uSFF) 4. Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu 5. Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM

	<ol style="list-style-type: none"> 6. Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany 7. Definiowanie statusów dla sprzętu (Nowy, Do kasacji, W serwisie, itd.) 8. Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc.) 9. Odczyt informacji o module TPM 10. Odczyt D3Dscore z WinSAT 11. Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: Switch, Router, Access Point, Bridge, Modem, NAS, UPS, itd.) 12. Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu 13. Automatyczne wykrywanie i tworzenie monitorów (producent, numer seryjny, rozdzielczość, odczyt firmy, działu, osoby odpowiedzialnej, głównego użytkownika) 14. Automatyczne tworzenie zestawów: Komputer + Monitor 15. Automatyczne utworzenie zestawów: Komputer + drukarka lokalna 16. Automatyczne utworzenie zestawów: host + maszyny wirtualne 17. Automatyczne wykrywanie czy komputer jest maszyną wirtualną 18. Wykrywanie maszyn wirtualnych typu: Parallels Virtual Platform 19. Określanie informacji o wykorzystywanej wirtualizacji 20. Podgląd zestawów, do których należy zasób 21. Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami 22. Przypisywanie stałego atrybutu COA, który będzie uwzględniany na raportach wyposażenia i audytu 23. Definiowanie szczegółowych informacji finansowych 24. Obsługa walut w danych finansowych 25. Definiowanie bazy dostawców sprzętu i oprogramowania 26. Automatyczne odczytywanie ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu) 27. Automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta 28. Agent odczytuje identyfikator SID komputera 29. Określanie adresu interfejsu webowego urządzenia sieciowego 30. Określanie typu gwarancji dla zasobu 31. Określenie wpływu biznesowego wybranego zasobu 32. Tworzenie własnych typów gwarancji 33. Określanie ikony dla typów zasobów 34. Integracja z Dell API 35. Wyszukiwanie i identyfikacja duplikatów zasobów 36. Geolokalizacja komputerów z agentem.
Raporty zasobów	<ol style="list-style-type: none"> 1. Raport dodanych załączników 2. Automatyczne tworzenie historii zmian sprzętu 3. Raport zbiorczy historii zmian w sprzęcie 4. Ewidencja zdarzeń serwisowych 5. Dodawanie notatek\komentarzy dla zdefiniowanych obiektów zasobów 6. Informacja na temat pojemności dysków twardych oraz wolnego miejsca 7. Wydruk\dodawanie jako załącznik protokołu przekazania\zwrotu\utyliczacji sprzętu 8. Wydruk\dodawanie jako załącznik protokołu przekazania dla całego zestawu 9. Kreator szablonów wydruków WYSIWYG 10. Definiowanie dedykowanych profili protokołów 11. Zapisywanie protokołów podczas generowania jako załącznik do zasobu 12. Wydruk\dodawanie jako załącznik Karty informacyjnej do elementu wyposażenia

	<ol style="list-style-type: none"> Wydruk lub zapis do pliku raportów ze szczegółami sprzętu Porównywarka wyników skanowania sprzętu Dzienniki zdarzeń systemu Windows Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu Geolokalizacja komputerów z agentem.
Zarządzanie zasilaniem	<ol style="list-style-type: none"> Zdalne włączanie i wyłączenie komputerów Obsługa SecureOn przy WakeOnLan Tworzenie harmonogramów wyłączenia i włączania komputerów Wybór 5 trybów zamknięcia systemu: Blokada komputera, Uśpienie, Hibernacja, Wyłączenie, Wymuszenie wyłączenia, Restart Możliwość anulowania /wyświetlenia komunikatu jeśli jest zalogowany użytkownik Możliwość przerwania / odłożenia zadania na żądanie użytkownika Wymuszenie wylogowania użytkownika przed wyłączeniem komputera Raport zadań jednorazowych oraz harmonogramów Monitoring obciążenia CPU
Funkcje dodatkowe	<ol style="list-style-type: none"> Zdalne wykonywanie skryptów (batch/powershell) - Obsługa zadań jednorazowych i cyklicznych Podpisywanie skryptów Powershell certyfikatem Wykonywanie skryptów w kontekście sesji użytkownika lub usługi Skrypty wykonywane po uruchomieniu komputera lub zalogowaniu użytkownika Wykonywanie zadań dla wszystkich komputerów Edytor skryptów z funkcją kolorowania składni Wykorzystywanie predefiniowanych skryptów Import informacji o wyposażeniu z pliku CSV Wyszukiwanie sterowników, informacji o komputerze, informacji o gwarancji w bazie producenta (DELL) Mechanizm automatycznego tworzenia rekordów producenta sprzętu (na podstawie wyników skanowania sprzętu) Generowanie kodów paskowych, QR dla każdego elementu wyposażenia Obsługa kodów QR Archiwum zasobów Przeniesienie utylizowanego wyposażenia do archiwum Automatyczne usunięcie informacji sieciowych oraz licencji agenta dla zasobu archiwizowanego Zarządzanie sprzętem przez aplikacje mobilną Powiadomienia o kończącej się gwarancji\umowie serwisowej dla zasobu Zachowanie ostatniego skanu sprzętu podczas konserwacji bazy danych Powiadomienia o utworzeniu monitora, wykryciu maszyny wirtualnej Grupowa zmiana atrybutów Personalizacja statusów zasobów
Zarządzanie oprogramowaniem	
Licencje	<ol style="list-style-type: none"> Inwentaryzacja licencji Automatyczne tworzenie licencji na podstawie kluczy produktów Odczytu OriginalProductKey (BIOS/UEFI) dla systemu operacyjnego Import licencji z pliku tekstowego Automatyczne generowanie historii zmian w licencji Określanie statusu licencji Tworzenie własnych atrybutów licencji Tworzenie notatek oraz załączników w dowolnym formacie do licencji

	<ol style="list-style-type: none"> 9. Tworzenie licencji z poziomu rozliczenia audytu legalności 10. Tworzenie licencji z poziomu raportu kluczy licencji 11. Tworzenie zestawów licencji 12. Relacja licencji z użytkownikiem, firmą, działem, lokalizacją 13. Zmiana typu licencji dla wybranej grupy 14. Kompletna informacja na temat posiadanych licencji (typ, producent, program licencjonowania, czas ważności, informacje finansowe) 15. Przypisywanie licencji do komputera 16. Definiowanie wymaganych atrybutów legalności (faktura, nośnik, COA, etc.) 17. Definiowanie ilości posiadanych licencji w rozbiu na użytkowników oraz stanowiska 18. Definiowanie licencji przeznaczonych do przyszłego zakupu 19. Definiowanie kluczy seryjnych i przypisywanie do licencji 20. Automatyczne usunięcie wiązania pomiędzy zasobem archiwizowanym a licencją 21. Określenie wpływu biznesowego wybranej licencji
Skanowanie oprogramowania	<ol style="list-style-type: none"> 1. Skanowanie oprogramowania na podstawie harmonogramu oraz definicji skanera 2. Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecenia skanów 3. Śledzenie zmian w stanie zainstalowanego oprogramowania 4. Zdalny skan komputerów (bieżący lub okresowy) 5. Zmiana priorytetu skanowania oprogramowania 6. Skan komputerów niepodłączonych do sieci 7. Wysyłanie wyników skanowania offline na serwer FTP (Audyt) 8. Przekazywanie konfiguracji wzorcowej dla skanera offline 9. Identyfikacja zainstalowanych aplikacji na podstawie wzorców oprogramowania 10. Prawidłowe rozpoznanie aplikacji nawet mimo zmiany jej nazwy 11. Określanie masek plików dla publikacji elektronicznych (e-book) 12. Skan plików skompresowanych 13. Skan oraz identyfikacja zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lz, lzma, msi, nrg, rar, tar, taz 14. Wbudowane profile skanowania (np. profil wzorcowy) 15. Definicja własnych ustawień skanowania 16. Porównywanie wyników skanowania oprogramowania 17. Wykrywanie plików multimedialnych 18. Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika) 19. Odczytywanie informacji o składnikach aplikacji, których programy instalacyjne nie są zgodne ze standardem MSI 20. Identyfikacja SID użytkownika, dla którego zainstalowano oprogramowanie 21. Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji\pakietów\systemów operacyjnych 22. Nadpisanie bazy wzorców najnowszą, oficjalną bazą producenta 23. Definiowanie katalogów wykluczonych / uwzględnionych w skanowaniu z wykorzystaniem symboli wieloznacznych (* , %)
Audyt oprogramowania	<ol style="list-style-type: none"> 24. Rozliczanie pakietów aplikacji 25. Rozliczanie systemów operacyjnych 26. Rozliczanie licencji typu „Downgrade”, „Upgrade” oraz instalacji innego oprogramowania w ramach licencji

	<ol style="list-style-type: none"> 27. Audyt oprogramowania rozliczany automatycznie - informacja o stanie posiadanych licencji i faktycznie zainstalowanych programach z uwzględnieniem wybranych zestawów licencji. 28. Historia audytów (Wyniki audytów powinny być przechowywane w bazie danych pozwalając na historyczny dostęp celem porównania i generowania raportów). 29. Wsparcie procesu Audytu przez zaimportowanie materiału zdjęciowego i jego obróbkę. 30. Gotowe metryki audytowanego komputera - załącznik do protokołu przekazania stanowiska komputerowego (sprzęt + oprogramowanie). 31. Uwzględnianie w rozliczeniu oprogramowania liczby aktywacji zapisanej w szablonie licencji
Funkcje	<ol style="list-style-type: none"> 1. Mechanizm informujący o nowej bazie wzorców oprogramowania 2. Definiowanie własnych wzorców oprogramowania 3. Automatyczne tworzenie wzorców oprogramowania dla systemów operacyjnych 4. Automatyczne dodawanie informacji o wydawcy oprogramowania dla nowych wzorców, tworzonych na podstawie wyników skanowania 5. Wykrywanie kluczy/identyfikatorów programów 6. W przypadku aktywacji systemu Windows z użyciem serwera KMS, klucza MAK (Multiple Activation Keys) lub VLK (Volume License Keys) program powinien odczytywać przynajmniej 5 ostatnich znaków klucza 7. Odczytywanie informacji o częściowych kluczach pakietów Microsoft Office 8. Drukowanie lub zapisywanie do pliku raportów ze szczegółami oprogramowania 9. Zbiorcze raporty wyników skanowania oprogramowania - Pakiety, pliki, systemy operacyjne, kluczy zainstalowanych aplikacji 10. Raport z informacjami o pakietach oprogramowania uwzględniający parametry: przybliżona wielkość, adres strony internetowej, lokalizacja pliku instalacyjnego, architektura aplikacji, itd. 11. Raport z informacjami o systemach operacyjnych uwzględniający parametry: Data instalacji, Architektura systemu, Wersja kompilacji, itd. 12. "Wielkie raporty" (Możliwość utworzenia zbiorczych raportów obejmujących np. wszystkie przeskanowane pliki) 13. Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (*.msi) 14. Zdalna dezinstalacja oprogramowania 15. Utworzenie harmonogramu dezinstalacji oprogramowania 16. Generowanie skryptu deinstalacji aplikacji na podstawie otrzymanych wyników skanowania oprogramowania 17. Raport stanu oprogramowania antywirusowego, anty-szpiegowskiego oraz zapory sieciowej 18. Raport zainstalowanych aktualizacji systemu Windows
	Kontrola wykorzystania sprzętu i oprogramowania
Pozyskiwanie informacji o użytkownikach, zarządzanie widokami, funkcje ogólne	<ol style="list-style-type: none"> 1. Dane gromadzone dla konkretnych użytkowników (na bazie kont Windows) - jeden użytkownik może mieć przypisanych wiele kont Windows i pracować na różnych komputerach 2. Odczyt informacji o kontach lokalnych komputera, wraz z odczytem grup do, których konto należy 3. Grupowanie użytkowników z podziałem na jednostki organizacyjne w firmie (np. względem działów) 4. Określanie firmy do której należy użytkownik 5. Określanie przełożonego dla użytkownika

	<ol style="list-style-type: none"> Prezentacja 'stanu użytkownika' (obecny, nieobecny, nowy). Prezentacja 'statusu użytkownika' (Zatrudniony, zwolniony, itd.) Zarządzanie stanowiskami użytkowników Przeniesienie rekordu użytkownika do archiwum Funkcjonalności automatycznego generowania zmian rekordu użytkownika – Historia użytkownika Odczytywanie informacji o użytkownikach z Active Directory oraz AAD Pełna synchronizacja rekordów użytkowników (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory oraz AAD) Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień Podgląd zdjęcia przypisanego do użytkownika Przypisywanie do użytkownika załączników (pliki) Przypisywanie notatek do użytkownika Ewidencja zdarzeń przypisanych do użytkowników Automatyczne tworzenie działów na podstawie informacji odczytanych z Active Directory
Raporty	<ol style="list-style-type: none"> Analiza aktywności użytkowników Grupowanie danych według komputerów jeśli użytkownik wykorzystywał więcej niż jedno stanowisko Analiza zdarzeń sesji użytkownika (Logowanie, Wylogowanie, Zablokowanie, Odblokowanie, Nawiązanie połączenia RDP, Zakończenie połączenia RDP) Analiza przerw w pracy Analiza jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków) Analiza aktywności mikrofonu oraz kamery Analiza wykorzystania poszczególnych aplikacji w czasie Analiza czasu działania aplikacji, na pierwszym planie oraz sumarycznie Uwzględnienie lub wyłączenie z raportu aplikacji bez aktywności użytkownika Kategoryzacja danych czasu pracy (czas pozytywny, neutralny oraz negatywny). Statystyki najczęściej wykorzystywanych aplikacji Statystyki wykorzystania komputerów przez poszczególnych użytkowników Statystyki aktywności użytkownika i grup użytkowników Generowanie raportów z monitoringu użytkowników dla wybranego zakresu godzin Kontrola wydruków - historia zadań drukowania zainicjowanych przez poszczególnych użytkowników Kontrola wydruków - Monitoring wydruków obejmuje szczegółowe parametry (np. format papieru, orientację, skalowanie, itd.) Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz-b/kolor, dpi) Monitoring wydruków na drukarkach sieciowych Monitoring użytkowników stacji terminalowych Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.) Informacje o awariach, poczynaniach użytkowników: zakończonej aktualizacji, akcji podpięcia przenośnych dysków, włożenia płyt do napędów CD/DVD, śledzenie uruchomienia aplikacji przez użytkownika, monitoring informujący o małej ilości miejsca Raport zbiorczy historii zmian w rekordach użytkowników
Funkcje	<ol style="list-style-type: none"> Blokada niepożądanych aplikacji. Programy mogą być blokowane dla całej firmy lub tylko dla wybranych użytkowników. Autoryzacja nośników zewnętrznych na podstawie wykrytych urządzeń

	<ol style="list-style-type: none"> Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych Automatycznie budowana baza informacji o napędach zewnętrznych Blokada dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.) Odczyt i blokada urządzeń PTP/MTP Określanie praw dostępu w zależności od typu urządzenia, np. Pendrive, CD/ROM Komunikacja z użytkownikami (Skype, mail) bezpośrednio z zakładki Użytkownicy Informacje o ostatnio zalogowanych osobach na stacjach klienckich Automatyczne tworzenie licencji – Dodawanie do licencji użytkowników, którzy są głównymi użytkownikami komputera, na którym wykryto licencje Komentowanie przerw pracy Kategoryzacja przerwy w pracy na podstawie komentarza
	Kontrola wykorzystania Internetu
Funkcje	<ol style="list-style-type: none"> Blokada stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokada WWW po zawartości (ContentType) Blokada stron internetowych dla protokołu http \ https w najpopularniejszych przeglądarkach WWW Kategoryzacja stron internetowych Import stron WWW z pliku lub ze schowka Słowniki kategorii stron WWW Blokada dostępu do witryn zgodnie z harmonogramem Blokada trybu incognito w przeglądarce Google Chrome
Raporty	<ol style="list-style-type: none"> Raporty dotyczące aktywności użytkowników w Internecie Analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki) Monitoring stron internetowych dla protokołu http \ https (Edge, Chrome, Opera, Vivaldi, Firefox) Analiza liczby wejść na poszczególne strony lub domeny Kategoryzacja odwiedzanych domen i stron Raport informujący o plikach pobranych przez przeglądarki WWW Raport informujący o danych wysłanych przez przeglądarki (bez Firefox) Monitoring plików pobieranych przez przeglądarki internetowe
	Helpdesk
Obsługa	<ol style="list-style-type: none"> Rejestracja i obsługa zgłoszeń Obsługa zgłoszeń w modelu Kanban Określanie relacji pomiędzy zgłoszeniami (np.. Kopia, Incydent nadrzędny) Edycja zgłoszeń powiązanych w oknie zgłoszenia bieżącego Kategoria zgłoszeń może posiadać swojego opiekuna, który może zarządzać każdym zgłoszeniem danej kategorii Komentarze zgłoszenia obsługujące HTML oraz osadzanie obrazów Opis zgłoszenia w formacie HTML Nawiązywanie połączeń zdalnych bezpośrednio z edytora incydent Tworzenie notatek dla zgłoszeń Zapisywanie wersji roboczej komentarza Archiwizacja zgłoszeń Monitoring czasu pracy nad incydem (time tracking) Raport ewidencji czasu pracy nad zgłoszeniem Informacja o czasie reakcji do podjęcia zgłoszenia

	<ol style="list-style-type: none"> 15. Dodanie prywatnego komentarza 16. Znaki @ oraz # pozwalają na wspomnianie użytkownika oraz wpisu bazy wiedzy w komentarzu zgłoszenia 17. Dodanie załączników do incydentów, również do komentarza 18. Określanie dodatkowych subskrybentów dla notyfikacji e-mail dotyczącej zmian w incydencie 19. Określanie uprawnień do incydentów (Publiczne, Prywatne, dla określonych działów) 20. Zarządzanie filtrami zdefiniowanymi dla listy zgłoszeń 21. Obsługa nazwy DNS oraz adresów IP (IPv4, IPv6) dla zgłoszeń 22. Wydruk historii zgłoszenia 23. Widok kalendarza (Planowanie rozwiązania incydentów) 24. Korelacja incydentu z elementem zasobów 25. Raport zbiorczy historii zmian 26. Tworzenie i planowanie zastępstw, osoba zastępująca otrzymuje na czas zastępstwa dostęp do obsługi zgłoszeń osoby zastępowanej 27. Wyszukiwanie komentarzy przy użyciu funkcji globalnego wyszukiwania 28. Czas reakcji oraz realizacji wyznaczany automatycznie na podstawie umów SLA 29. Automatyczne podpowiedzi rozwiązań dostępnych w bazie wiedzy na podstawie wpisywanego tematu 30. Określenie wpływu biznesowego wybranego zgłoszenia 31. Podgląd wiadomości źródłowej przy tworzeniu zgłoszenia lub komentarza na podstawie zgłoszeń email 32. Duplikacja i replikacja zgłoszeń 33. Powiadomienia o liczbie nieprzeczytanych zgłoszeń 34. Automatyzacja obsługi zgłoszeń z wykorzystaniem utworzonych reguł
Konfiguracja	<ol style="list-style-type: none"> 1. Architektura drzewa dla kategorii zgłoszeń 2. Tworzenie szablonów odpowiedzi 3. Cykliczne raportowanie Listy incydentów 4. Tworzenie własnych dodatkowych atrybutów dla zgłoszeń 5. Personalizowane szablony wiadomości email z możliwością ustawienia stałego załącznika 6. Notyfikacje e-mail o utworzeniu\zmianie\usunięciu incydentu 7. Notyfikacje e-mail o zbliżających się terminach realizacji incydentu (Deadline) 8. Automatyczny import wiadomości e-mail, jako zgłoszeń helpdesk (POP3 oraz IMAP) 9. Import zgłoszeń helpdesk ze skrzynek współdzielonych (shared mailbox) 10. Obsługa wielu kont pocztowych (Import + notyfikację email) 11. Tworzenie własnych trybów oraz priorytetów incydentów 12. Personalizacja widoku raportu listy incydentów 13. Profile zgłaszających w helpdesk 14. Personalizacja kolorów statusów zgłoszeń 15. Automatyczne przypisywanie zgłoszeń do użytkowników 16. Weryfikacja wiadomości źródłowych pobieranych z serwera pocztowego 17. Konfiguracja maksymalnej wielkości załącznika
Moduł połączeń zdalnych	<ol style="list-style-type: none"> 1. Operacje na plikach i katalogach 2. Zarządzanie procesami i rejestrem 3. Monitoring pracy wykonywanej na komputerze 4. Zdalny podgląd pulpitów wielu stacji w miniaturach ekranów 5. Wywoływanie Windows Remote Desktop na danej stacji z poziomu aplikacji 6. Wysyłanie wiadomości do użytkowników 7. Uruchamianie na stacjach programów z wiersza poleceń Command Line 8. Zdalne uruchamianie komputera za pomocą funkcji Wake-On-Lan

	<ol style="list-style-type: none"> Wake-On-Lan pozwala na definicję portu oraz adresu komputera docelowego Przejęcie kontroli nad stacją roboczą Blokada klawiatury i myszki na stacji klienckiej w trakcie przejęcia kontroli pulpitu zdalnego Przesyłanie kombinacji klawiszy Ctrl + Alt + Delete w zdalnym pulpicie Przejęcie kontroli nad komputerem bez zalogowanego użytkownika Wysyłanie pytania o zgodę na zdalny dostęp lub wysyłania komunikatu z informacją o rozpoczęciu podglądu pulpitu Podgląd pulpitu zdalnego w osobnym oknie z opcją fullscreen Obsługa wielu monitorów dla podglądu pulpitu Wybór monitora, z którego ma być przekazywany obraz podglądu pulpitu Nawiązywanie połączenia pulpitu zdalnego z wieloma komputerami jednocześnie Połączenie pulpitem zdalnym w konfiguracji NAT-NAT Zarządzanie usługami systemu Windows Raport Sesje zdalnego pulpitu Wybór adresu IP, na którym ma być zestawione połączenie zdalne Wybór portu, na którym klient nasłuchuje połączenia zdalnego Wykorzystanie protokołu autorskiego lub MS RDP do połączeń zdalnych
Baza wiedzy	<ol style="list-style-type: none"> Wbudowana baza wiedzy Artykuły bazy wiedzy mogą być przypisane do kategorii zgłoszeń helpdesk Kopiowanie artykułów Edytor HTML Osadzanie załączników w treści artykułów Osadzanie multimediów w treści artykułów Baza wiedzy pozwala na tworzenia artykułów prywatnych oraz publicznych Szybkie kopiowanie wpisów bazy wiedzy Artykuły bazy wiedzy mogą zostać powiązane ze zgłoszeniami z systemu helpdesk Artykuły bazy wiedzy mogą zostać przypięte, dzięki czemu zawsze będą widoczne na liście artykułów Informacja o liczbie odsłon artykułu bazy wiedzy Bezpośrednie linkowanie artykułów bazy wiedzy
SLA	<ol style="list-style-type: none"> Definiowanie planów umów SLA Definiowanie czasu obowiązywania umów SLA Definiowanie czasu pracy działów wsparcia technicznego Definiowanie dni wolnych na podstawie kalendarza świąt i dni wolnych Definiowanie czasów reakcji oraz realizacji zgłoszenia Notyfikacje mailowe o zbliżających się terminach reakcji oraz realizacji Automatyczne przypisanie umowy SLA do zgłoszenia na podstawie informacji o rozwiązującym, temacie wiadomości, priorytecie, kategorii, opisie Raportowanie o statusie i postępie w realizacji zgłoszeń z przypisaną umową SLA
Centralne repozytorium załączników	
Funkcje	<ol style="list-style-type: none"> Załączniki przechowywane w centralnym repozytorium Utworzenie relacji załącznika z innymi elementami systemu 1 - N (jeden do wielu) Dodawanie i modyfikacja załączników z poziomu innych zasobów Załączniki typu: link, udział oraz plik Pełna informacja o załączniku: twórca, data utworzenia, rozmiar, nazwa pliku, miniatura

	6. Historia zmian załącznika
	Zarządzanie użytkownikami
Funkcje	<ol style="list-style-type: none"> 1. Raportowanie aktywności pracy 2. Przeglądanie ostatnio zgłoszonych incydentów 3. Powiązanie użytkownika z licencją 4. Dostęp webowy do statystyk monitoringu, zgłoszeń helpdesk oraz powiązanych z użytkownikiem zasobów 5. Cykliczne, automatyczne generowanie raportów 6. Generowanie raportu obecności / nieobecności użytkownika wraz z korelacją jego aktywności na komputerze 7. Zgłoszenia dotyczące wniosków nieobecności użytkowników 8. Automatyczne typowanie użytkowników zastępujących dla zgłaszanych nieobecności 9. Zarządzanie wnioskami nieobecności użytkowników przez przełożonych, informowanie przełożonych N poziomów wyżej o urlopie użytkownika 10. Automatyczne utworzenie relacji przełożony - podwładny na podstawie skanów Active Directory 11. Możliwość drukowania karty informacyjnej użytkownika, zawierającej informacje kontaktowe, informacje o powiązanych zasobach, licencjach oraz dostępy nadane w module RODO 12. Generator struktury organizacji na podstawie powiązań użytkowników i ich przełożonych 13. Planowanie dni wolnych w widoku kalendarza 14. Planowanie zastępstw podczas nieobecności
	Raportowanie cykliczne
Użytkownicy	<ol style="list-style-type: none"> 1. Raport historia sesji 2. Raport Nośniki danych 3. Raport Operacje na plikach 4. Raport wydruków 5. Raport użycia aplikacji 6. Raport nagłówków okien 7. Raport odwiedzonych stron WWW 8. Najczęściej odwiedzane strony internetowe 9. Raport Wysyłane pliki 10. Raport czasu pracy przy komputerze 11. Raport zestawienia kategoryzacji czasu pracy przy komputerze
Zasoby	<ol style="list-style-type: none"> 1. Raport historii zasobów 2. Raport informujący o nowych zasobach 3. Raport informujący o nadchodzących terminach w zasobach 4. Raport Zasoby zarchiwizowane 5. Raport Systemy Operacyjne
Podstawowe	<ol style="list-style-type: none"> 1. Raport Informacje o autoryzowanych agentach
Oprogramowanie	<ol style="list-style-type: none"> 1. Raport zainstalowanego oprogramowania 2. Raport Szczegóły plików
Helpdesk	<ol style="list-style-type: none"> 1. Raport incydentów (Helpdesk) 2. Raport czasu pracy nad zgłoszeniem 3. Raport Cząsy SLA

Automatyzacja	
Ogólne	<ol style="list-style-type: none"> 1. Wygaśnięcie certyfikatu SSL 2. Kończące się licencje na agenta 3. Zapełniona baza danych 4. Zbyt duży rozmiar folderu cache
Zasoby	<ol style="list-style-type: none"> 1. Brak połączenia od agenta 2. Brak wolnej przestrzeni na dysku 3. Ostrzeżenie od Windows Security Center 4. Zakończenie skanowania sprzętu 5. Dodanie zasobu 6. Zmiana zasobu 7. Usunięcie zasobu 8. Zakończenie okresu gwarancyjnego 9. Zakończenie umowy serwisowej 10. Powielenie zasobów
Oprogramowanie	<ol style="list-style-type: none"> 1. Zmiana oprogramowania 2. Zakończenie skanowania oprogramowania 3. Zamknięcie audytu
Licencje	<ol style="list-style-type: none"> 1. Dodanie licencji 2. Zmiana licencji 3. Usunięcie licencji 4. Wygaśnięcie licencji 5. Planowana wymiana licencji
Użytkownicy	<ol style="list-style-type: none"> 1. Dodanie użytkownika 2. Zmiana użytkownika 3. Usunięcie użytkownika 4. Logowanie użytkownika 5. Wylogowanie użytkownika
Helpdesk	<ol style="list-style-type: none"> 1. Dodanie zgłoszenia 2. Usunięcie zgłoszenia 3. Zmiana zgłoszenia 4. Brak aktywności w zgłoszeniu
Lista dostępnych Akcji	<ol style="list-style-type: none"> 1. Wykonywanie skryptu na podstawie zdefiniowanej reguły 2. Wysłanie powiadomienia w konsoli zarządzającej na podstawie zdefiniowanej reguły 3. Wysyłanie powiadomienia mailowego na podstawie zdefiniowanej reguły (inicjator zdarzenia, Administratorzy, konkretny użytkownik, rozwiązujący, zgłaszający, subskrybenci) 4. Modyfikacja zasoby / użytkownika / zgłoszenia - w zależności od reguły 5. Dodanie komentarza (dla reguł Helpdesk) 6. Wysyłka wiadomości SMS
RODO	
Funkcje	<ol style="list-style-type: none"> 1. Inwentaryzacja zbiorów danych, dostępów oraz powierzeń do zbiorów danych, dokumentów bezpieczeństwa, historii naruszeń bezpieczeństwa, szkoleń oraz wniosków o zapomnienie

	<ol style="list-style-type: none"> 2. Wydruk raportów tabelarycznych: czynności przetwarzania,ostępów, powierzeń, listy dokumentów, statystyki zgłoszeń RODO, listę szkoleń, historii naruszeń bezpieczeństwa, wniosków o zapomnienie 3. Wydruk wniosków o nadanie uprawnień, modyfikacji oraz anulowania upoważnienia 4. Wstępne wypełnienie wniosków o zmianę dostępu 5. Utworzenie zgłoszeń za pomocą przycisków szybkiej akcji 6. Delegowanie zadań w helpdesk dla osób odpowiedzialnych za zbiory danych 7. Archiwizacja zbiorów 8. Definiowanie czynności przetwarzania 9. Przypisywanie zbioru danych do czynności przetwarzania 10. Przydzielanie dostępów do czynności przetwarzania 11. Zapisywanie historii zmian wniosków o dostęp do zbiorów 12. Dodawanie historycznych dostępów oraz wniosków o dostęp 13. Filtrowanie użytkowników w raporcie Dostęp
Raporty	<ol style="list-style-type: none"> 1. Raport zbiorczy Czynności przetwarzania 2. Raport zbiorczy Zbiory danych 3. Raport zbiorczy zinwentaryzowanych dostępów 4. Raport zbiorczy zinwentaryzowanych powierzeń 5. Raport zbiorczy zinwentaryzowanych dokumentów 6. Raport zbiorczy historii naruszeń bezpieczeństwa 7. Raport zbiorczy wniosków o dostęp 8. Raport zbiorczy Dostęp
RODO	
Funkcje	<ol style="list-style-type: none"> 1. Inwentaryzacja zbiorów danych, dostępów oraz powierzeń do zbiorów danych, dokumentów bezpieczeństwa, historii naruszeń bezpieczeństwa, szkoleń oraz wniosków o zapomnienie 2. Wydruk raportów tabelarycznych: czynności przetwarzania,ostępów, powierzeń, listy dokumentów, statystyki zgłoszeń RODO, listę szkoleń, historii naruszeń bezpieczeństwa, wniosków o zapomnienie 3. Wydruk wniosków o nadanie uprawnień, modyfikacji oraz anulowania upoważnienia 4. Wstępne wypełnienie wniosków o zmianę dostępu 5. Utworzenie zgłoszeń za pomocą przycisków szybkiej akcji 6. Delegowanie zadań w helpdesk dla osób odpowiedzialnych za zbiory danych 7. Archiwizacja zbiorów 8. Definiowanie czynności przetwarzania 9. Przypisywanie zbioru danych do czynności przetwarzania 10. Przydzielanie dostępów do czynności przetwarzania 11. Zapisywanie historii zmian wniosków o dostęp do zbiorów 12. Dodawanie historycznych dostępów oraz wniosków o dostęp 13. Filtrowanie użytkowników w raporcie Dostęp
Raporty	<ol style="list-style-type: none"> 1. Raport zbiorczy Czynności przetwarzania 2. Raport zbiorczy Zbiory danych 3. Raport zbiorczy zinwentaryzowanych dostępów 4. Raport zbiorczy zinwentaryzowanych powierzeń 5. Raport zbiorczy zinwentaryzowanych dokumentów 6. Raport zbiorczy historii naruszeń bezpieczeństwa 7. Raport zbiorczy wniosków o dostęp 8. Raport zbiorczy Dostęp

Sygnalista	
Funkcje	<ol style="list-style-type: none"> 1. Tworzenie zgłoszeń w postaci anonimowej lub nieanonimowej 2. Usuwanie metadanych z załączników zgłoszeń 3. Usuwanie danych osobowych ze zgłoszeń 4. Podział interfejsu na publiczny oraz dla wewnętrzny 5. Dashboard podsumowujący wykorzystanie portalu sygnalisty 6. Przypisywanie rozwiązujących zgłoszenia sygnalistów w zależności od typu zgłoszenia lub jego źródła 7. Definiowanie własnych atrybutów, kategorii, trybów zgłoszeń oraz poziomów ryzyka 8. Definiowanie stron publicznych (dostępnych dla sygnalistów) 9. Obsługa wielu języków stron publicznych 10. Natywne wsparcie języka ukraińskiego 11. Definiowany limit załączników 12. Wyróżnienie zgłoszeń o przekroczonym czasie reakcji
Raporty	<ol style="list-style-type: none"> 1. Raport zgłoszeń 2. Historia zmian 3. Statystyka zgłoszeń 4. Pozostały czas na przyjęcie zgłoszenia 5. Pozostały czas do zakończenia 6. Widżety: Kategorie zgłoszeń, Poziomy ryzyka, Tryby zgłoszeń, Statusy zgłoszeń, Ostatnio dodane
Portal Web	
Funkcje	<ol style="list-style-type: none"> 1. Wallboard - ekran zbiorczy prezentujący wybrane informacje z całego systemu 2. Dashboard każdego modułu z najważniejszymi informacjami w postaci widżetów 3. Widok zawierający oś czasu z aktywnością użytkownika 4. Rozbudowane filtry dla raportów tabelarycznych 5. Zarządzanie użytkownikami, agentami, zasobami, licencjami, działami, audytami 6. Konfiguracja portalu helpdesk, kont administracyjnych oraz organizacji 7. Raporty dla każdego modułu w formie tabelarycznej 8. Obsługa helpdesk oraz bazy wiedzy 9. Obsługa modułu RODO 10. Obsługa modułu automatyzacja 11. Obsługa kanału zgłoszeń wewnętrznych dla Sygnalistów 12. Automatyczne logowanie przy pomocy aplikacji 13. Logowanie za pomocą poświadczeń domenowych (SSO) 14. Logowanie za pomocą konta AzureAD lub AAD 15. Wydruk raportów tabelarycznych 16. Kontrola statystyk użytkowników 17. Menu szybkiego dodawania nowych elementów (użytkownik, nieobecność, zasób, licencja, zgłoszenie, artykuł bazy wiedzy, zbiór danych, czynność przetwarzania) 18. Przełączanie wersji językowej bez ponownego logowania do systemu 19. Nawigacja Breadcrumb
Funkcjonalności ogólne	
<ol style="list-style-type: none"> 1. Określanie praw dostępu do grup zasobów lub użytkowników 	

2. Aplikacja desktopowa służąca do zarządzania systemem może być zainstalowana na dowolnej liczbie komputerów ("Licencja pływająca")
3. Dodatkowa aplikacja webowa umożliwiająca dostęp do systemu i zarządzanie systemem
4. Wersja angielska (en-US) interfejsu użytkownika
5. Praca w oparciu o silniki baz danych: MS SQL lub PostgreSQL
6. Swobodna migracja danych pomiędzy MS SQL i PostgreSQL
7. Zdalna instalacja i dezinstalacja agentów na stacjach roboczych
8. Odczytywanie struktury organizacji z Active Directory
9. Skaner sieci wykorzystywany do wykrywania nowych urządzeń
10. Mechanizm automatycznego tworzenia komputera na podstawie danych przesłanych przez agenta
11. Mechanizm automatycznego tworzenia użytkowników na podstawie danych przesłanych przez agenta
12. Automatycznie dodane komputery/użytkowników są powiązane z odpowiednią grupą zgodną z OU w Active Directory
13. Definiowanie nieograniczonej liczby użytkowników systemu
14. Określanie ról dla kont systemu na przykład Administratorzy, Menadżerowie, Zarządcy, Pracownicy
15. Indywidualny login i hasło dla poszczególnych użytkowników
16. Automatyczne logowanie do systemu
17. Zarządzanie uprawnieniami użytkowników - określanie dostępu do poszczególnych obiektów systemu (konkretny użytkownik, konkretny zasób lub ich grupy) , możliwość ograniczenia operacji (wyświetlanie, tworzenie, edycja, usuwanie)
18. Dostęp do programu chroniony przy pomocy uwierzytelniania wieloskładnikowego
19. Określanie ról użytkowników - zarządzanie grupami
20. Zabezpieczenie Agentów przed nieautoryzowanym wyłączeniem lub usunięciem
21. Eksport danych do plików zewnętrznych (Excel, html, CSV, PDF, TXT, MHT, RTF, BMP)
22. Zgodny z pracą w sieciach WLAN
23. Podgląd aktualnych zadań serwera
24. Centrum informacji - przekrojowy raport na temat zdarzeń oraz statusu monitorowanych komputerów i użytkowników
25. Wielopoziomowe drzewo lokalizacji oraz relacje lokalizacji z firmami
26. Wyszukiwanie danych w tabelach raportów
27. Dowolne definiowanie grup sprzętu i użytkowników
28. Tworzenie dowolnych raportów ad-hoc - sortowanie kolumn grupowanie, ukrywanie/odkrywanie kolumn, zaawansowane filtrowanie danych w oparciu o funkcje logiczne
29. Definiowanie i zapamiętywanie własnych widoków
30. Eksport danych bezpośrednio do MS Excel
31. Budowa zestawień metodą drag'n'drop
32. Budowa modułowa z możliwością przypisywania określonych wtyczek programu (funkcji) do poszczególnych Agentów
33. Obsługa protokołu SSL zapewniającego bezpieczną komunikację Master-Serwer oraz Agent-Serwer.
34. Połączenia pomiędzy komponentami realizowane za pomocą HTTP/HTTPS lub net.TCP
35. Mechanizm kompresji pakietów danych przesyłanych przez Agenta
36. Automatyczne wykrywanie lokalizacji serwera aplikacji (WS-Discovery)
37. Przekazanie agentowi nowych parametrów połączenia z usługą serwera (serwer zapasowy)
38. Definiowanie konfiguracji serwera proxy dla połączenia Agent-Serwer
39. Mechanizm zdalnego pobierania bieżących aktualizacji do programu
40. Help kontekstowy wraz z podręcznikiem użytkownika w polskiej wersji językowej
41. Dostęp do bazy wiedzy systemu
42. Definiowanie ustawień pracy Agentów (optymalizacja dla dużej liczby komputerów)
43. Dedykowane narzędzie, dostarczane z systemem, do wykonywania kopii bazy danych, niezależnie od wersji silnika bazy danych (MSSQL, PostgreSQL). Uruchomienie narzędzia backupu bazy w trybie wsadowym
44. Manualna i automatyczna konserwacja bazy danych - usuwanie wyników skanowania oprogramowania
45. Personalizacja pakietu instalacyjnego agenta
46. Określanie polityki haseł dla systemu
47. Zmiana języka systemu podczas logowania

48. Określenie numeru BDO przy definiowaniu rekordu firmy
49. Opcja resetu hasła podczas logowania
50. Globalne wyszukiwanie obiektów w systemie
51. Utworzenie atrybutów jako lista/słownik
52. Podgląd aktualnie zalogowanych użytkowników. Umożliwienie wylogowania wybranych użytkowników
53. Definicja kalendarzy dni wolnych, uwzględnianych w module Helpdesk oraz Monitoring
54. Wyszukiwarka ustawień w opcjach systemowych
55. Instalacja konsoli zarządzającej w kontekście użytkownika (nie wymaga uprawnień administracyjnych)
56. Historia obiektu zawiera informacje o koncie serwisowym, które wprowadziło zmianę w obiekcie
57. Skanowanie lasu domen
58. Budowa personalizowanego pakietu instalacyjnego
59. Automatyczne zamknięcie konsoli zarządzającej po zakończeniu sesji
60. Logowanie do portalu Web za pomocą mechanizmu Single Sign On
61. Logowanie operacji kont serwisowych
62. Dodatkowa metoda uwierzytelniania klientów przed połączeniem do serwera
63. Logowanie nieudanych prób uwierzytelnienia
64. Eksport danych diagnostycznych oraz dzienników operacji
65. Integracja z SMS API

Dodatkowe informacje

1. Kreator instalacyjny ułatwiający wdrożenie systemu
2. Aplikacja dla wersji 64 bity OS
3. Rozproszona architektura systemu: Serwer, konsola zarządzająca, Agent (Możliwa praca każdego z komponentów na różnych komputerach)
4. Praca w oparciu o MS SQL Server oraz MS SQL Express (2008/2012/2014/2016/2019/2022 32/64 bit)
5. Praca w oparciu o PostgreSQL 16 lub nowszy
6. Szyfrowane połączenie pomiędzy serwerem aplikacji, a bazą danych
7. Obsługa systemów operacyjnych - **Agent**: Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, Windows 10, Windows 11
8. Obsługa systemów operacyjnych – **konsola zarządzająca** : Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, Windows 10, Windows 11
9. Obsługa systemów operacyjnych - **Serwer**: Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, Windows 10, Windows 11
10. Wszystkie wykonywalne komponenty systemu powinny być podpisane certyfikatem **DigiCert Code Signing Certificates for Microsoft Authenticode (Digicert)**
11. Sterowniki systemowe powinny być podpisane certyfikatem **Extended Validation (EV) Code Signing Certificate (GlobalSign)** i mogą pracować w 64-bitowych systemach operacyjnych Microsoft Windows™.