Załącznik nr 8 do SWZ – Szczegółowy opis przedmiotu zamówienia

Specyfikacja warunków zamówienia

I część: dostawa sprzętu komputerowego

1. Serwer – szt 1

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	Charakterystyka ogólna	Serwer będzie przeznaczony do instalacji oprogramowania zwiększającego poziom cyberbezpieczeństwa w środowisku Zamawiającego. Na serwerze będą instalowane i dostępne narzędzia do ochrony sieci, takie jak system do skanowania aktywów Zamawiającego, inwentaryzacja sieci , systemy DLP do ochrony przed wyciekiem danych, domena do zarzadzania siecią i zwiększenie wpływów nad zarzadzaniem użytkownikami . Jego przeznaczenie to ochrona infrastruktury IT przed zagrożeniami, zarządzaniem dostępem do zasobów oraz zapewnieniem bezpieczeństwa
2.	**Obudowa**	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5” Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
3.	**Płyta główna**	Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 32 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Na płycie głównej powinno znajdować się minimum 16

		slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
4.	**Chipset**	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
5.	**Procesor**	Zainstalowane dwa procesory 12-rdzeniowy, min. 2.0GHz, umożliwiający osiągnięcie wyniku min. 214 w teście SPECrate2017_int_base, dla oferowanego serwera, dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej
6.	**RAM**	Minimum 256GB DDR5 RDIMM 5600MT/s, ECC osiągnięte za pomocą 4 modułów 64GB
7.	**Funkcjonalność pamięci RAM**	Demand Scrubing, Patrol Scrubing, Permanent Fault Detection
8.	**Gniazda PCI**	minimum dwa sloty PCIe
9.	**Interfejsy sieciowe/FC/SAS**	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
10.	**Dyski twarde**	Zainstalowane: 3x dysk SSD SATA o pojemności min. 960GB, 6Gbps, 2,5“ Hot-Plug. 2x dysk M.2 NVME o pojemności min. 480GB
11.	**Kontroler RAID**	Sprzętowy kontroler dyskowy, posiadający Min. 8GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących
12.	**Moduł NVME do instalacji systemu operacyjnego**	Karta rozszerzeń umożliwiająca instalację systemu operacyjnego na redundantnych dyskach NVMe M.2 w konfiguracji RAID 1. PCIe Gen3 x4 lub złącze dedykowane zgodne z architekturą serwera. Obsługiwane dyski: Minimum 2 × NVMe M.2. Obsługa RAID: RAID 1.
13.	**Wbudowane porty**	4 x USB z czego nie mniej niż 1x USB 3.0, 2x VGA
14.	**Video**	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200

15.	**Zasilacze**	Redundantne, Hot-Plug min. 700W klasy Titanium
16.	**Elementy montażowe**	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
17.	**System operacyjny**	Microsoft Windows Server 2022 Standard lub równoważny spełniający min. poniższe wymagania: Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i minimum dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading; Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

		Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. Możliwość migracji konfiguracji systemu Microsoft Windows Serwer 2021/2016.
18.	**Licencje dostępowe**	Licencje dostępowe CAL , dla użytkowników w ilości 40 szt.
19.	**Bezpieczeństwo**	Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem

		Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
20.	**Karta Zarządzania**	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: zdalny dostęp do graficznego interfejsu Web karty zarządzającej; zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; możliwość podmontowania zdalnych wirtualnych napędów; wirtualną konsolę z dostępem do myszy, klawiatury; wsparcie dla IPv6; wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; integracja z Active Directory; możliwość obsługi przez dwóch administratorów jednocześnie; wsparcie dla dynamic DNS; wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej Przesyłanie danych telemetrycznych w czasie rzeczywistym Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze Automatyczna rejestracja certyfikatów (ACE)
21.	**Oprogramowanie do zarządzania**	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:

		Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych integracja z Active Directory Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram Szczegółowy opis wykrytych systemów oraz ich komponentów Możliwość eksportu raportu do CSV, HTML, XLS, PDF Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. Grupowanie urządzeń w oparciu o kryteria użytkownika Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach Szybki podgląd stanu środowiska Podsumowanie stanu dla każdego urządzenia Szczegółowy status urządzenia/elementu/komponentu Generowanie alertów przy zmianie stanu urządzenia. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń Integracja z service desk producenta dostarczonej platformy sprzętowej Możliwość przejęcia zdalnego pulpitu Możliwość podmontowania wirtualnego napędu Kreator umożliwiający dostosowanie akcji dla wybranych alertów Możliwość importu plików MIB Przesyłanie alertów „as-is” do innych konsol firm trzecich Możliwość definiowania ról administratorów Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta Możliwość automatycznego

		generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. Zdalne uruchamianie diagnostyki serwera. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
22.	**Certyfikaty**	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO14001 Serwer musi posiadać deklaracja CE. Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z

		co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
23.	**Dokumentacja użytkownika**	Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
24.	**Wsparcie techniczne i oprogramowanie** – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego, automatycznie tworzące zgłoszenia serwisowe w przypadku awarii. Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera. Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów. Konfiguracja i zaoferowany poziom wsparcia powinien po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia powinien się kontaktować z klientem w celu rozwiązania problemu. Oprogramowanie musi współpracować z kartą do zarządzania w urządzeniu, która będzie działać niezależnie od zainstalowanego systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit. Karta musi umożliwiać

		podmontowanie zdalnych wirtualnych napędów, oraz wirtualną konsolę z dostępem do myszy, klawiatury. Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające : Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień. Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów. Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta. upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji : o poprawkach i usprawnieniach dotyczących aktualizacji dacie wydania ostatniej aktualizacji priorytecie aktualizacji zgodność z systemami operacyjnymi jakiego komponentu sprzętu dotyczy aktualizacja wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (ddmm-rrrr) sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla

		oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm- rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.

2. UTM - **ZAPORA SIECIOWA UTM OCHRONA STYKU SIECI LAN /WAN - szt 2**

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	Wymagania Ogólne	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. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzwanego dytrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. 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. System wspiera protokoły IPv4 oraz IPv6 w zakresie: Firewall. Ochrony w warstwie aplikacji. Protokołów routingu dynamicznego. Redundancja, monitoring i wykrywanie awarii

		W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. Interfejsy, Dysk, Zasilanie: System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 5 portami Gigabit Ethernet RJ-45. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. System jest wyposażony w zasilanie AC. Parametry wydajnościowe: W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 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 1 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps. Systemu Bezpieczeństwa: W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: Kontrola dostępu - zapora ogniowa 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, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). Polityki, Firewall 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: 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. 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. Amazon Web Services (AWS). Microsoft Azure.

		Cisco ACI. Google Cloud Platform (GCP). OpenStack. VMware NSX. Kubernetes. Połączenia VPN System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: Wsparcie dla IKE v1 oraz v2. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). Obsługa protokołu Diffie-Hellman grup 19, 20. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. 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 zasobó wsystemu. 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. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: 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 łączy WAN W zakresie routingu rozwiązanie zapewnia obsługę: Routingu statycznego. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).

		Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. BFD (Bidirectional Forwarding Detection). Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. Funkcje SD-WAN System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). Zarządzanie pasmem System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. System daje możliwość określania pasma dla poszczególnych aplikacji. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. Ochrona przed malware Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 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. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

		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. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. Ochrona przed atakami Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. Kontrola aplikacji Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

		Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 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 Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 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. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 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. Uwierzytelnianie użytkowników w ramach sesji System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: 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 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 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, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 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 Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, bazy reputacyjne adresów IP/domen na okres [24 miesięcy. Gwarancja oraz wsparcie System jest objęty serwisem gwarancyjnym producenta przez okres [12] miesiące 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. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie zamawiającego, realizowana przez producenta lub autoryzowanego dystrybutora w języku polskim przez okres wymaganej gwarancji. Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji. Do zamawianego sprzętu Wykonawca zapewni usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie: obsługa procesu RMA u producenta, zdalna pomoc w skonfigurowaniu urządzenia do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producenta, jednorazowa podstawowa konfiguracja platformy realizowana przez inżyniera z najwyższym dostępnym poziomem certyfikacji technicznej producenta, dostęp do szkolenia wideo prezentującego najlepsze praktyki współpracy z suportem producenta systemu realizującego funkcję Firewall.

		Dostęp do usługi powinien być świadczony przez dedykowaną infolinię (należy podać numer telefonu) oraz przez dedykowany moduł internetowy (należy podać adres). Usługa ta ma być świadczona prze podmiot posiadający certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Do oferty należy załączyć oświadczenie producenta lub Autoryzowanego Dystrybutora o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001 oraz certyfikat potwierdzający posiadany najwyższy poziom certyfikacji technicznej producenta . Rozszerzone wsparcie serwisowe AHB/SOS a) System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesiące Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7 System producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie: Wsparcie telefoniczne zespołu certyfikowanych inżynierów. Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu jest objęty usługą wsparcia technicznego świadczoną przez. Doradztwo w zakresie konfiguracji. Zdalne wsparcie techniczne. Pomoc w zakładaniu zgłoszeń serwisowych u producenta. Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). Przygotowanie urządzenia do zdalnej konfiguracji. Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich. Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia

		serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym. Wymagania powinny być potwierdzone dokumentami: Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). Certyfikat ISO 9001 podmiotu serwisującego. Załączyć do oferty

3. macierz dyskowa – 1 szt + dyski – 6 szt

Lp.	Parametr	Wymagania minimalne
1.	Obudowa	Do instalacji w standardowej szafie RACK 19” z kompletem szyn przesuwnych w zestawie. Macierz musi zajmować wysokość maksymalnie 2U i pozwalać na instalacje min. 12 dysków. Nie dopuszcza się zastosowania rozwiązania złożonego z macierzy wraz z jednostką rozszerzającą o takiej samej wysokości maksymalnej.
2.	Rozbudowa	Do minimum 440 dysków poprzez dołożenie jednostek rozszerzających.
3.	Obsługiwane dyski	Minimum: • 2.5" 12Gb/s SAS SSD, • 2.5" 12Gb/s SAS 10,000 RPM HDD, • 3.5" 12Gb/s NL-SAS 7,200 RPM HDD. Macierz musi umożliwiać zastosowanie dysków rożnych producentów bez ograniczeń do dysków tego samego producenta co macierz (brak tzw. „vendor lock”).
4.	Zainstalowane dyski	Minimum 6 dysków zgodnych z listą kompatybilności oferowanej macierzy oraz charakteryzujących się następującymi parametrami: • pojemność: minimum 3.84TB, • odczyt sekwencyjny: do 4000 MB/s, • zapis sekwencyjny: do 3500 MB/s, • losowy odczyt: do 760 tys. IOPS, • losowy zapis: do 130 tys. IOPS, • interfejs: SAS 12Gb/s lub SAS 24Gb/s, • gwarancja: minimum 60 miesięcy,

		• wytrzymałość: minimum 1 DWPD.
5.	Kontrolery	Dwa sprzętowe kontrolery pracujące w trybie active-active.
6.	Cache kontrolera	Minimum 16GB DDR4 ECC z możliwością rozbudowy do minimum 128GB.
7.	Zabezpieczenie pamięci cache	Moduł podtrzymania pamięci cache oparty o kondensator wraz dyskiem flash, który w przypadku awarii zasilania macierzy zabezpieczy dane przechowywane w pamięci podręcznej cache, które nie zostały zapisane na dyskach.
8.	Wentylatory	Wentylatory lub moduły wentylatora z możliwością wymiany podczas pracy macierzy.
9.	Zasilanie	Redundantny zasilacz o mocy minimalnej pozwalającej na bezproblemową pracę macierzy w przypadku awarii jednego modułu zasilacza, potwierdzony certyfikatem sprawności 80 PLUS Platinum lub wyższym.
10.	Obsługiwane typy RAID	Minimum RAID 0, 1, 5, 6, 10, 50, 60
11.	Interfejsy kontrolera	Minimum: • 1 port 1GbE RJ-45 LAN (zarządzanie), • 2 porty 12Gb SAS 12Gb/s (do podłączania jednostek rozszerzających) • 4 porty 10GbE SFP+ iSCSI (z kompletem modułów 10Gb/s SFP+ SR)
12.	Rozbudowa interfejsów kontrolera	Możliwość zamontowania dodatkowych rozszerzeń, minimum: • 4 portowych 10GbE SFP+ iSCSI, • 2 lub 4 portowych 25GbE SFP28 iSCSI, • 2 lub 4 portowych 16Gb SFP+ Fibre Channel, • 2 portowych 32Gb SFP28 Fibre Channel.
13.	Oprogramowanie i funkcjonalności	• Migawki blokowe (minimalnie 4096 migawek na cały system), • Thin provisioning z odzyskiwaniem miejsca, • zdalna replikacja asynchroniczna, • zdalna replikacja synchroniczna (opcja), • Konfiguracja Quality of Service (QoS), • Automatyczne warstwowanie danych (opcja), • Pamięć podręczna SSD Cache (opcja), • Obsługa LACP, Multi-pathing, Trunking oraz Jumbo frame, • wsparcie dla RESTful API. Jeżeli którakolwiek funkcjonalność wymaga aktywacji poprzez dodatkową licencję wymagana jest możliwość zakupu takiej licencji osobno po zakupie

		macierzy. Nie jest wymagane dostarczenie licencji na etapie dostawy macierzy.
14.	Wsparcie dla systemów operacyjnych i środowisk wirtualizacji	Minimum Windows Server 2022, VMware vSphere ESXI 8
15.	Certyfikaty	CE, Macierz musi być wyprodukowana zgodnie z normą ISO 9001:2015 i ISO 14001:2015.
16.	Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
17.	Gwarancja	Minimum 36 miesięcy gwarancji Next Business Day producenta. W przypadku potwierdzonej awarii sprzętowej dostarczone zostaną sprawne, pojedyncze elementy macierzy (np. moduł zasilacza, kontroler). Wymianę uszkodzonych podzespołów realizuje klient we własnym zakresie. Obowiązuje od poniedziałku do piątku w dni robocze. Nie dotyczy dysków. Wymagana jest możliwość sprawdzenia typu i ważności gwarancji, a także szczegółowej konfiguracji sprzętowej poprzez dedykowaną stronę producenta. Strona ta po podaniu unikalnego numeru identyfikacyjnego macierzy powinna udostępniać informacje dotyczące modelu macierzy, wersji oprogramowania, zamontowanych dodatkowych kart rozszerzeń, pamięci RAM, aktywowanych licencji oraz modelu i wersji oprogramowania zainstalowanych dysków HDD i SSD.

4. zarządzane urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X – 2 szt.

1	Cechy zarządzania	Warstwa przełącznika: L2/L3 Obsługa jakości usług (QoS): Tak Zarządzanie przez stronę WWW: Tak Inspekcja ARP: Tak Porty Poe: Tak Konfigurowanie ustawień lokalizacji (CLI): Tak Obsługa MIB: Tak
2	Porty i interfejsy	Liczba portów Ethernet RJ-45: 48 Liczba portów PoE: 48 Typ portów Ethernet RJ-45: Gigabit Ethernet (10/100/1000) Liczba zainstalowanych modułów SFP+: 4

	Sieć	Obsługiwane standardy: IEEE 802.1Q, IEEE 802.1ab, IEEE 802.1ad, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ad, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z Dublowanie portów: Tak Blokowanie head-of-line (HOL): Tak Prędkość transferu danych: 1000 Mbit/s Kontrola wzrostu natężenia ruchu: Tak Protokół drzewa rozpinającego: Tak Podpora kontroli przepływu: Tak Obsługa sieci VLAN: Tak Obsługa Multicast: Tak
	Przesyłanie danych	Trasa statyczna: Tak Zgodność z Jumbo Frames: Tak Rozszerzenie Jumbo Frames: 9000
	Ochrona	Lista kontrolna dostępu (ACL): Tak IGMP snooping: Tak Obsługa SSH/SSL: Tak Szyfrowanie / bezpieczeństwo: HTTPS, SSH, SSL/TLS Filtrowanie adresów MAC: Tak
	Konstrukcja	Kolor: Biały Materiał obudowy: Metal Przycisk reset: Tak Diody LED: Tak Szerokość: 350 mm Głębokość: 444,5 mm Wysokość: 43,9 mm
	Wydajność	Taktowanie procesora: 1400 MHz Pamięć wewnętrzna: 1024 MB Wielkość pamięci flash: 512 MB
	Zasilanie	Źródło zasilania: Prąd przemienny Typ wtyczki: Typu C
	Oprogramowanie	Dostęp do najnowszych aktualizacji firmware bezpośrednio ze strony producenta

II część – dostawa oprogramowania

5. oprogramowanie do monitorowania infrastruktury informatycznej z licencją na 50 stanowisk– 1 szt – wymagany okres obowiązywania licencji – 12 m-cy

1	Architektura / budowa	1.1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 50 Klientów jednocześnie. 1.2. Architektura / budowa: 1.2.1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej. 1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). 1.2.3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach. 1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami. 1.2.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej. 1.3. Konfiguracja Architektury: 1.3.1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie. 1.3.2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.
2.	2.Wymagania systemowe	2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera). 2.2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa. 2.2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2 2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11.

		2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9. 2.5. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych bezpłatnym (np. Microsoft SQL Server Express Edition). 2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.
3.	Interfejsy	3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie. 3.2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL 3.3. System zapewnia integrację z modelem LLM.
4.	Funkcjonalności systemu zarządzania infrastrukturą IT	4.1. Funkcjonalność Klienta 4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku. 4.2. Funkcjonalność konsoli administracyjnej. 4.2.1. Konsola administracyjna musi być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie. 4.2.2. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.

		4.2.3. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń. 4.3. Funkcjonalność panelu pracownika 4.3.1. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora. 4.4. Zarządzanie licencjami 4.4.1. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania. 4.5. Wzorce aplikacji i pakietów 4.5.1. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office. 4.6. Inwentaryzacja sprzętu komputerowego i urządzeń. 4.6.1. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń. 4.7. Inwentaryzacja urządzeń sieciowych. 4.7.1. System musi posiadać zdolności do identyfikacji oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci. 4.8. Inwentaryzacja sprzętu.

		4.8.1. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych. 4.9. Ochrona danych (DLP) 4.9.1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami. 4.10. Szyfrowanie dysków wewnętrznych oraz zewnętrznych 4.10.1. System musi obsługiwać kompleksowe szyfrowanie dysków wewnętrznych i zewnętrznych USB, z wykorzystaniem BitLocker i różnych metod szyfrowania, takich jak XTS_AES_256 i AES_128. Musi umożliwiać zdalne zarządzanie procesem szyfrowania/deszyfrowania, w tym masowe operacje na partycjach systemowych i niesystemowych, zarówno lokalnie, jak i zdalnie (poza NATem). Klucze szyfrujące są przechowywane i chronione w konsoli administracyjnej, dostępne tylko po uwierzytelnieniu administratora. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika i nie może być przez niego przerwany, z wyjątkiem stanów hibernacji i wyłączenia systemu, po których jest automatycznie kontynuowany. 4.11. Zdalna administracja komputerami 4.11.1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia. 4.12. System musi umożliwiać zdalne w technologii WEBRTC. 4.12.1. System musi zapewniać zdalne zarządzanie komputerami przy użyciu technologii WEBRTC, umożliwiając jednoczesne połączenia z wieloma urządzeniami. Powinien oferować funkcje takie jak przejęcie kontroli nad pulpitami, zarządzanie plikami, uruchamianie i zarządzanie aplikacjami oraz

		instalowanie oprogramowania i aktualizacji. System powinien umożliwiać konfigurację połączeń WEBRTC, w tym instalację i konfigurację odpowiednich serwerów i portów. Dodatkowo, system powinien obsługiwać różne tryby przejęcia sesji, włączając opcje z lub bez zgody użytkownika, a także umożliwiać nagrywanie i zarządzanie sesjami połączeń, w tym wykonywanie zrzutów ekranu i nagrywanie sesji. System powinien również wspierać różnorodne konfiguracje wyświetlania i jakości sesji, a także umożliwiać uruchomienie do 12 sesji na jednym ekranie. 4.13. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia. 4.14. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu. 4.15. Zdalna instalacja 4.15.1. System musi umożliwiać zdalną instalację pakietów MSI i plików .exe, korzystając z Windows Management Instrumentation (WMI) oraz usługi Klient bez dodatkowych poświadczeń, wykorzystując lokalne i sieciowe repozytoria. Powinien obsługiwać tworzenie repozytorium instalatorów z możliwością dodawania aplikacji, zarządzania wersjami oraz kategoryzacji. System musi również umożliwiać tworzenie grup instalacyjnych, definiowanie schematów instalacyjnych i automatyzację procesu instalacji na nowych urządzeniach. Powinien zawierać kiosk aplikacji umożliwiający użytkownikom samodzielną instalację aplikacji oraz rejestrować i raportować wszystkie procesy instalacji, umożliwiając również ich przerwanie. 4.16. Zdalne Zarządzanie Zaporą (Firewall) 4.16.1. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe. 4.17. Automatyzacja 4.17.1. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT. 4.18. Zarządzanie magazynem IT

		4.18.1. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów. 4.19. Repozytorium 4.19.1. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją. 4.20. Kody kreskowe 4.20.1. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych. 4.21. Wysyłanie wiadomości 4.21.1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania. 4.22. System musi posiadać możliwość eksportu / importu treści. 4.23. Monitorowanie drukarek sieciowych i wydruków 4.23.1. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych. 4.24. Monitorowanie stron www 4.24.1. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a

		także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści. 4.25. Monitorowanie serwerów WWW 4.25.1. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie. 4.26. Monitorowanie dziennika zdarzeń 4.26.1. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii. 4.27. System musi umożliwiać monitorowanie komunikatów Syslog. 4.28. Monitorowanie pracy komputerów 4.28.1. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników. 4.29. Monitorowanie sensorów 4.29.1. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów. 4.30. Repozytorium CMDB 4.30.1. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych. 4.31. Worktime manager 4.31.1. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostepnienia w panelu pracownika. 4.32. Raportowanie i eksport danych 4.32.1. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów.

		Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu. 4.33. System musi zapewnić interfejs API. 4.33.1. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki. 4.34. Powiadomienia 4.34.1. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji. 4.35. Bezpieczeństwo 4.35.1. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.
5.	Wsparcie i pomoc	5.1.1. Pomoc techniczna 5.1.1.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00. 5.1.1.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania. 5.1.1.3. Czas trwania usługi SLA wynosi do 30.06.2026 r. od dnia zakupu.

6. oprogramowanie przeciwdziałające wyciekowi danych z licencja na 50 stanowisk – 1 szt.
Wymagany okres obowiązywania licencji – 12 m-cy

1.	Architektura / budowa	1.1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 50 Klientów jednocześnie. 1.2. Architektura / budowa: 1.2.1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej. 1.2.1.1. Połączenie klient – serwer, Komunikacja odbywa się z wykorzystaniem TLS 1.2.1.2. Serwer i klient posiadają certyfikaty SSL (4096 bitowe). 1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych). 1.2.3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach zgodnie ze specyfikacją opisaną poniżej. 1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami. 1.2.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej. 1.3. Konfiguracja Architektury: 1.3.1. Komponenty Klient, konsola administracyjna, serwer, baza danych muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu. 1.3.2. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja Klientów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania

		aktualizacji manualnie poprzez pobranie od producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją. 1.3.3. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, polityk, pomoc i inne wbudowane bazy wiedzy. 1.3.4. Klient do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI. 1.3.5. Klient musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku *.msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku *.msi. 1.3.6. Klient musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej. 1.3.7. System zapewnia możliwość stworzenia instalatora (.exe) z wbudowanymi, zaszyfrowanymi poświadczeniami dla dowolnego konta. Funkcja ta umożliwia instalację usługi bezpośrednio na kontach użytkowników – zarówno lokalnych, jak i domenowych, korzystając z uprawnień zdefiniowanych dla instalatora w konsoli systemu. 1.3.8. Klient musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa). 1.3.9. System powinien umożliwiać generowanie unikatowego identyfikatora Klienta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków. 1.3.10. Klient musi mieć definiowalny priorytet pracy (ABOVE_NORMAL, NORMAL, BELOW_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów. 1.3.11. Klient musi wspierać wiele różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu Klienta. 1.3.12. System musi umożliwiać komunikację pomiędzy Klientami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.

		1.3.13. System musi mieć możliwość współpracy komponentów Klient i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami Klientów. 1.4. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem. 1.4.1. Automaty powinny realizować co najmniej: 1.4.1.1. Usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nie przyrostowe, zmniejszanie bazy danych. 1.4.2. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie.
2.	Wymagania systemowe	2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera). 2.2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa. 2.2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2 2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11. 2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9. 2.5. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych bezpłatnym (np. Microsoft SQL Server Express Edition). 2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.
3.	Interfejsy	3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym

		import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie. 3.1.1. Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID. 3.1.2. Import z Active Directory musi wspierać obsługę protokołów SSL oraz TLS. 3.1.3. Import z Active Directory musi umożliwiać podanie więcej niż jednej domeny. 3.2. System musi umożliwiać import użytkowników z zewnętrznego pliku CSV. 3.3. System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switche itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane. 3.4. System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS. 3.5. System zapewnia integrację z modelem LLM.
4.	Funkcjonalność systemu	4.1. Funkcjonalność Klienta 4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania Klienta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego). 4.1.2. Klient musi mieć możliwość konfiguracji zakresu skanowania plików. 4.1.3. Klient musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej, konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkowniku, który go wyświetlił. 4.2. Funkcjonalność konsoli administracyjnej. 4.2.1. Konsola musi być w pełni polskojęzyczna. 4.2.2. Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie).

		4.2.3. Konsola administracyjna musi posiadać dashboard – dashboard użytkownika, dashboard prezentujący parametry infrastruktury, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie. 4.2.4. Konsola administracyjna musi być wyposażona w panel zawierający graficzne widżety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi. 4.2.5. Dane na widżetach muszą być aktualizowane automatycznie. 4.2.6. System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widżety, ich konfigurację i kolejność). 4.2.7. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu. 4.2.8. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą mieć możliwość filtrowania kolumnowego. 4.2.9. System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji. 4.2.10. Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu. 4.2.11. Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko). 4.2.12. Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja Klienta, stanu Klienta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera. 4.2.13. Konsola musi zawierać w sobie pełną dokumentację systemu. 4.3. Odczytywanie zainstalowanego oprogramowania 4.3.1. System powinien prezentować podgląd zainstalowanych systemów operacyjnych, pakietów oraz aplikacji na komputerach z informacjami o: nazwie, wersji, producencie, typie licencji. 4.4. Wzorce aplikacji i pakietów

		4.4.1. System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 4 tys. wzorców aplikacji, 1,3 tys. Producentów. 4.4.2. System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania. 4.4.3. Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów. 4.4.4. System musi mieć możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera / komputerów wzorce mają być utworzone. Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu. 4.5. Inwentaryzacja sprzętu komputerowego 4.5.1. System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem). 4.5.2. System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language. 4.5.3. System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu). 4.5.4. System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania. 4.5.5. System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza począwszy od wskazanego miejsca w hierarchii kluczy rejestru. 4.5.6. System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu). 4.5.7. System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).

		4.5.8. System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku. 4.5.9. System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu. 4.5.10. System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent). 4.5.11. System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne. 4.5.12. System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów. 4.5.13. System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik) 4.5.14. System umożliwia dodawanie notatek do każdej pozycji sprzętu. 4.5.15. System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części). 4.5.15.1. System musi umożliwiać definiowanie typów serwisów 4.5.15.2. System musi umożliwiać definiowanie wartości serwisu 4.5.15.3. System musi umożliwiać definiowanie daty ważności serwisu oraz daty gwarancji 4.5.16. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium. 4.5.17. System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja). 4.6. Inwentaryzacja urządzeń podłączanych do komputera. 4.6.1. System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.) 4.6.2. System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika. 4.6.3. System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika). 4.7. Inwentaryzacja urządzeń sieciowych. 4.7.1. System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym IP/porcie i zwracać

		podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać SNMP w wersji 1/2c/3. 4.7.2. Skaner SNMP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port. 4.7.3. System musi zbierać informacje o jakości połączenia: 4.7.4. Czas odpowiedzi serwisów (usług) podawany w milisekundach: 4.7.4.1. Średni czas odpowiedzi. 4.7.4.2. Minimalny czas odpowiedzi. 4.7.4.3. Maksymalny czas odpowiedzi. 4.7.5. Ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat. 4.7.6. System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają Klienta. 4.7.6.1. Posiada niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci 4.7.6.2. Baza wzorców musi zawierać ponad 100 monitorowanych portów i usług. 4.7.6.3. System musi umożliwiać administratorowi definiowanie dodatkowych portów do monitorowania i przypisywanie do nich usług, a także modyfikowanie istniejących rekordów, obejmujących: port TCP, kategorię, nazwę usługi oraz nazwę skróconą. 4.7.7. System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci. 4.7.7.1. System musi umożliwiać generowanie map według dowolnych filtrów użytkownika. 4.8. Zdalna administracja komputerami 4.8.1. System ma automatyczne wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika. 4.8.1.1. System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu Windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania.

		4.8.1.2. Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory Windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego. 4.8.1.3. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status). 4.8.1.4. System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, Windows PowerShell. System posiada co najmniej 70 predefiniowanych poleceń. System musi umożliwiać użytkownikom automatyczne definiowanie poleceń cmd/PowerShell. Funkcjonalność ta pozwala na wprowadzanie opisów zadanych czynności, a następnie, wykorzystując zaawansowane algorytmy AI, system automatycznie generuje adekwatne skrypty. 4.8.1.5. Zaawansowany Asystent AI do Przygotowywania Skryptów do precyzyjnego tworzenia szczegółowych skryptów 4.8.1.6. System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.). 4.8.1.7. System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako) 4.8.1.8. System musi umożliwiać tworzenie zadań cyklicznych dla komputerów. 4.8.1.9. Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/drugi/trzeci/czwarty/ostatni poniedziałek/wtorek/środa/czwartek/piątek/sobota/niedziela/dzień wolny/dzień powszedni co n miesięcy, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania.

		4.8.1.10. System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie. 4.8.2. System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro. 4.8.2.1. System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączanie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji. 4.8.2.2. System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6). 4.8.3. System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacja oprogramowania, poprawek i aktualizacji (service pack, patch). 4.8.3.1. System umożliwia zdalne podłączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii Ultra VNC. 4.8.3.2. System musi umożliwiać uruchomienie do 6 sesji Ultra VNC na jednym ekranie. 4.8.3.3. System musi umożliwiać uruchomienie sesji Ultra VNC w trybie podłączenia się do obecnie zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejęcia dostępu). 4.8.4. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia. 4.8.5. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu. 4.9. Wysyłanie wiadomości 4.9.1. Komunikator 4.9.1.1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości pomiędzy użytkownikiem komputera z zainstalowanym Klientem a administratorem systemu. 4.9.1.2. Powinien zapewniać możliwość inicjowania czatu przez administratora. 4.9.1.3. Użytkownik powinien mieć opcję rozpoczęcia rozmowy za pomocą ikony na pasku zadań, która automatycznie uruchamia się zgodnie z konfiguracją Klienta. 4.9.1.4. System musi przechowywać historię konwersacji.

		4.9.1.5. Powinien informować administratora poprzez powiadomienie w konsoli systemowej o nowych wiadomościach od użytkowników. 4.9.2. Wiadomość Jednorazowa: 4.9.2.1. System powinien umożliwiać wysyłanie jednorazowych wiadomości w trybie natychmiastowym jako ALERT. 4.9.2.2. Musi oferować możliwość wysłania wiadomości z opcją odłożenia na później (na 10 minut, 1, 2, 4 godziny) dla późniejszego odczytu. 4.9.2.3. Powinien zapewniać historię wysyłania i odbierania wiadomości przez użytkowników, z możliwością edycji treści w edytorze HTML. 4.9.2.4. Wiadomość powinna być dostępna do wysłania do określonej grupy, wybranych komputerów lub użytkowników. 4.9.2.5. System musi umożliwiać konfigurację czasu wygaśnięcia wiadomości. 4.9.3. Wiadomości Cykliczne: 4.9.3.1. Powinien pozwalać na tworzenie szablonów wiadomości do regularnego użytku. 4.9.3.2. Musi zapewniać funkcję odłożenia wysyłania wiadomości dla późniejszego odczytu, z możliwością edycji treści w edytorze HTML. 4.9.3.3. System powinien rejestrować historię wysyłania i odczytywania wiadomości przez użytkowników. 4.9.3.4. Powinien umożliwiać wysłanie wiadomości do zdefiniowanej grupy, wybranych komputerów lub użytkowników. 4.9.3.5. Musi oferować opcję konfiguracji terminu, po którym wiadomość wygaśnie. 4.9.4. System szkolenia pracowników za pomocą wiadomości. 4.9.4.1. System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów. 4.9.4.2. System musi posiadać predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa”, „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa”, „Postępowanie w przypadku naruszenia tajemnicy”, „Udostępnienie informacji stanowiących tajemnicę”. 4.9.4.3. Formatowanie treści musi być zgodne z HTML. 4.9.4.4. System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych). 4.9.4.5. System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców. 4.9.4.6. Użytkownik otrzymujący wiadomość musi być powiadamiany wizualne i dźwiękowo o otrzymaniu nowej wiadomości.

		4.9.4.7. Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania. 4.9.4.8. System musi udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników. 4.9.4.9. System musi generować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem). 4.10. Repozytorium CMDB 4.10.1.1. System musi posiadać wbudowaną centralną bazę systemu umożliwiająca import i eksport niektórych danych zarówno poprzez API jak też za pomocą wbudowanego import/eksporta. 4.11. Worktime manager 4.11.1. System musi być wyposażony w zestaw statystycznych danych o pracy użytkownika i zdefiniowanych grup użytkowników. 4.11.2. System musi umożliwiać definiowanie dowolnej ilości grup użytkowników przypisanych do dowolnej ilości przełożonych. 4.11.3. System musi umożliwić wyświetlanie informacji o użytkowniku pobranych z Active Directory. Informacje powinny być aktualizowane zgodnie z harmonogramem połączenia z domeną. 4.12. Zarządzanie politykami bezpieczeństwa. 4.12.1. System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez bieżące (w czasie rzeczywistym) monitorowanie działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa oraz reguł ich opisujących. 4.12.2. System musi zapewniać automatyczne uruchamianie ochrony zasobów w czasie rzeczywistym zgodnie ze zdefiniowanymi politykami. 4.12.3. System musi zapewniać ciągłą ochronę danych niezależnie od położenia komputera (w sieci lokalnej, sieci VPN, poza siecią). 4.12.4. System musi na bieżąco monitorować i chronić za pomocą odpowiednio zdefiniowanych polityk i reguł dane w ruchu, dane w spoczynku oraz dane w użyciu. 4.12.5. Przez dane w spoczynku rozumie się dane, które nie są (ale mogą być) w ruchu lub w użyciu, wymagają inwentaryzacji i zabezpieczenia. 4.12.6. Przez dane w użyciu należy rozumieć dane, które są aktywnie przetwarzane przez dowolną aplikację i/lub punkt końcowy (komputer). Przykłady danych w użyciu: edycja dokumentu MS Word, Excel, PowerPoint, edycja pliku tekstowego CSV, TXT, tworzenie pliku, przechwytywanie ekranu (screenshot), kopiowanie / wklejanie danych. 4.12.7. Przez dane w ruchu należy rozumieć dane, które są przesyłane, np. kopiowanie danych (plików) z dysku sieciowego na nośnik USB, kopiowanie

		danych (plików) z komputera na komputer, przesyłanie danych e-mailem w treści lub w postaci załącznika, pobieranie danych z serwera FTP, przesyłanie danych za pomocą komunikatora. 4.12.8. Obiekty docelowe reguł muszą być definiowalne za pomocą parametrów takich jak: nazwa komputera, adres IP, unikatowy identyfikator agenta, status podłączenia do systemu (online/offline), zainstalowany system operacyjny, nazwę zalogowanego użytkownika, model komputera, producent komputera, dostawca komputera, budżet, z którego zakupiony został komputer, strukturę organizacyjną 4.12.9. Przy definiowaniu obiektów docelowych dla reguł DLP można korzystać ze znaków wieloznacznych. 4.12.10. System musi posiadać funkcjonalności monitorowania, blokowania, powiadomieniu użytkownika o wystąpieniu naruszenia zdefiniowanej polityki oraz pełnego logowania zdarzeń dotyczących polityki dla celów administracyjnych (powiadomienie administratora systemu). 4.12.11. System musi mieć możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP. 4.12.12. System musi mieć możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji. 4.12.13. Nowy komputer zgłaszający się do systemu po raz pierwszy musi bez dodatkowej ingerencji administratora automatycznie pobrać oraz wdrożyć (uruchomić) przeznaczoną dla niego politykę. 4.12.14. System musi mieć możliwość określenia ram czasowych działania danej reguły. 4.12.15. System musi dysponować mechanizmami dostępu do plików na poziomie jądra systemu operacyjnego MS Windows (32-bit i 64-bit), co uniemożliwia obejście zabezpieczeń nawet osobie z uprawnieniami administratora na poziomie systemu operacyjnego. 4.13. System musi w pełni wspierać następujące polityki ochrony danych: 4.13.1. Zdefiniowanie schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione. 4.13.2. Monitorowanie wykonywanych zrzutów ekranu, blokowanie możliwości zapisania i wykorzystania zrzutów ekranu. 4.13.3. Przechwytywanie zrzutów ekranu z komputerów użytkowników wyzwalany akcją użytkownika lub na życzenie administratora zgodnie z wcześniej ustawionym interwałem czasowym.

		4.13.4. Umożliwienie powiadamianie o przekroczeniu dozwolonego czasu pracy komputera. 4.13.5. Wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku).
5.	Kontrola i ochrona urządzeń	5.1. Blokowanie dostępu do wybranych typów urządzeń od strony sprzętowej. Wsparcie dla CD-ROM, portów USB, kart sieciowych, GPS, kart graficznych, modemów, klawiatur, czytników kart, drukarek, urządzeń Bluetooth i innych, monitorowanie podłączanych urządzeń. 5.2. Blokowanie dostępu do urządzeń USB, tworzenie czarnych list urządzeń, monitorowane podłączanych urządzań USB. 5.3. Zarządzanie dostępem do sieci społecznościowych, serwisów informacyjnych, blogów, bibliotek, forów dyskusyjnych oraz dowolnych stron www. 5.3.1. Blokowanie sieci ze względu na zdefiniowany typ i maskę sieci WIFI. Polityka musi zapewniać blokowanie dostępu do sieci zarówno otwartych jak i zabezpieczonych.
6.	Klasyfikacja i ochrona dokumentów	6.1. Oznaczanie na dowolnym komputerze (znakowanie przez agenta) określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami. 6.2. Znakowanie określonych plików przechowywanych w zasobach serwerów lub udostępnionych zasobach (np. samodzielna macierz dyskowa) wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami, z wykorzystaniem harmonogramu. 6.3. Monitorowania i blokowania operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach.
7.	Ochrona danych w użyciu	7.1. Podjęcie działania w momencie uruchomienia określonego procesu. 7.2. Podjęcie działań monitorowania i blokowania operacji w momencie próby kopiowania tekstu, zdjęcia czy ścieżki plików do schowka.
8.	Ochrona danych w ruchu	8.1. Monitorowanie danych przesyłanych za pomocą poczty e-mail oraz blokowanie przesyłania plików określonych typów. 8.2. Monitorowanie danych przesyłanych do chmury oraz blokowanie synchronizacji plików określonych typów z wybraną chmurą.
9.	Raportowanie i eksport danych	9.1. System musi umożliwiać wyeksportowanie wybranych lub wszystkich danych do formatu .xls, .xlsx, .csv, .calc (OpenOffice), .html, .mht, .xml, .jpeg, .png, .gif, .bmp. 9.2. System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów, przy czym generowanie raportu musi odbywać się po stronie serwera www.

		9.3. System powinien umożliwiać eksport danych z raportu do formatów: pdf, xls, doc, rtf. 9.4. System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu). 9.5. System musi istnieć możliwość tworzenia i dodawania własnych raportów przez użytkownika.
10.	Bezpieczeństwo	10.1. System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej. 10.1.1. Uwierzytelnianie do systemu musi być realizowane: 10.1.1.1. z wykorzystaniem imiennego konta użytkownika i hasła, 10.1.1.2. z wykorzystaniem imiennego konta administratorów aplikacji i hasła, 10.1.1.3. za pośrednictwem uwierzytelniania poprzez Active Directory, 10.1.1.4. za pośrednictwem uwierzytelniania poprzez CAS, 10.1.2. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej. 10.1.3. Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków). 10.1.4. System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie (MFA). 10.1.4.1. Uwierzytelnianie z wykorzystaniem obrazu wideo. 10.1.4.2. Uwierzytelnianie z jednorazowym kodem wysyłanym na e-mail użytkownika. 10.1.4.3. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe wraz z hasłem, które umożliwia jednoczesną pracę wielu użytkownikom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory/LDAP. 10.1.5. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania w oparciu o RSA 512/1024/RSA 2048 bit, ECDSA 192/256 bit, DES/3DES, AES 128/192/256 bit, SHA-1 / SHA-256. 10.1.5.1. Wykorzystywane klucze muszą posiadać wsparcie dla systemów Windows 7/8.1/10 i Windows Server 2012/2016/2019. 10.1.6. System musi umożliwiać blokadę dostępu po nieudanej próbie zalogowania się do systemu. Ponadto, system powinien oferować:

		10.1.6.1. Podgląd wszystkich zablokowanych administratorów systemu, w tym informacje o typie, elemencie, czasie trwania blokady [s] oraz o ostatniej aktywności. 10.1.6.2. Możliwość odblokowania zablokowanego administratora systemu z poziomu konsoli administracyjnej przez osobę uprawnioną. 10.1.7. Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport. 10.1.8. System musi oferować możliwość podglądu wszystkich aktualnie otwartych sesji administratorów w konsoli administracyjnej, obejmując takie informacje jak: data utworzenia sesji, login, IP oraz SID. 10.1.8.1. Dodatkowo, system powinien umożliwiać wyszukiwanie zalogowanych administratorów po nazwie. 10.1.9. System musi udostępniać historię działań wybranych użytkowników/administratorów w zakresie, adresy URL i nagłówki http. 10.1.10. System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy Klientami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera. 10.1.11. System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nie przyrostowej oraz udostępniać informacje o rezultacie wykonania kopii. 10.1.12. System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych. 10.1.13. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy). 10.1.14. System musi być wyposażony w mechanizmy powtórnego załadowania danych historycznych pochodzących od Klientów. 10.1.15. System musi zapewniać: 10.1.15.1. Pełne logowanie błędów w celu weryfikowania nieprawidłowości. 10.1.15.2. Przechowywanie logów systemowych. 10.1.15.3. Przechowywanie logów bezpieczeństwa. 10.1.15.4. Przechowywanie logów aktywności użytkowników i administratorów. 10.1.15.5. Pobieranie logów z Klientów z poziomu konsoli administracyjnej. 10.1.15.6. Możliwość eksportu logów. 10.1.15.7. Definiowanie maksymalnego czasu przechowywania plików log. 10.1.15.8. System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.

		10.1.15.9. Definiowanie ścieżki do kopii zapasowej 10.1.15.10. Definiowanie ścieżki do importu danych 10.1.15.11. Definiowanie ścieżki do zapisu raportów 10.1.15.12. Definiowanie serwera do importu danych
11.	Wsparcie i pomoc	11.1.1. System musi posiadać dokumentację w postaci min. 5 filmów instruktażowych/nagrań z webinariów w języku polskim. 11.1.2. System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim. 11.1.3. Pomoc techniczna 11.1.3.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00. 11.1.3.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania. 11.1.3.3. Czas trwania usługi SLA wynosi do 30.06.2026 r. od dnia zakupu. 11.1.3.4. Usługi Utrzymania Oprogramowania obejmują: 11.1.3.4.1. asystę techniczną, 11.1.3.4.2. świadczenie usług SLA, w ramach, których realizowana jest: 11.1.3.4.2.1. obsługa zgłoszeń w zakresie: 11.1.3.4.2.1.1. reakcja na zgłoszenia błędów w określonym czasie reakcji; 11.1.3.4.2.1.2. dokonywanie analizy przyczyn błędów; 11.1.3.4.2.1.3. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich; 11.1.3.4.2.1.4. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie infrastruktury zamawiającego; 11.1.3.4.2.1.5. usuwania błędów w czasie naprawy; 11.1.3.4.2.1.6. usuwania błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich – po udostępnieniu odpowiedniej aktualizacji przez producenta tego oprogramowania oraz jej uzyskaniu – w czasie naprawy; 11.1.3.5. zapewnienia dostępności Oprogramowania.

7. Oprogramowanie antywirusowe z licencją na 50 stanowisk – 1 szt

Zamawiający posiada obecnie oprogramowanie ESET PROTECT Entry – 50 stanowisk – identyfikator publiczny: 3AA-T9R-6B7. Wskazana jest migracja do oprogramowania ESET PROTECT Enterprise – 50 stanowisk z zachowaniem obecnego klucza licencyjnego lub innego oprogramowania spełniającego wymagania Zamawiającego.

Zamawiający dopuszcza również rozwiązanie równoważne zgodne z poniższymi zapisami:

Zamawiający wymaga dostawy 50 licencji na okres 24 miesięcy zgodnych z poniższą specyfikacją. Ponadto zamawiający wymaga w przypadku dostarczenia oprogramowania równoważnego przeprowadzenia certyfikowanego przez producenta oprogramowania szkolenia dla administratora Urzędu, wdrożenia w siedzibie klienta, zainstalowania na wyznaczonych stacjach/serwerach/ urządzeniach mobilnych oraz przeniesienia konfiguracji z obecnie stosowanego systemu. Operacja ma się odbywać po godzinach pracy urzędu ze względu na potencjalne utrudnienia dla pracowników.

1	Administracja zdalna w chmurze	1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. 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. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. 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. 12. 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.
2	Ochrona stacji roboczych	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. 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. 22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. 23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: • 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 e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
3.	Ochrona serwera	Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux 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. Dodatkowe wymagania dla ochrony serwerów Windows: 9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 13. 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. 14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii

		w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe wymagania dla ochrony serwerów Linux: 18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 21. 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 zawieszonego mikro-serwisu.
3	Szyfrowanie	1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11. 2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 3. Aplikacja musi posiadać autentykacje 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
4	Ochrona urządzeń mobilnych opartych o	1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.

	system Android	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: a. usunięcie zawartości urządzenia, b. przywrócenie urządzenie do ustawień fabrycznych, c. zablokowania urządzenia, d. uruchomienie sygnału dźwiękowego, e. lokalizację GPS. 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła.
5	Sandbox w chmurze	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 przesyłać 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 lokalizacje 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 podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. 12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: a) Czysty, b) Podejrzany, c) Bardzo podejrzany, d) Szkodliwy. 13. W 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.

6	Moduł XDR	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. 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.

8. Oprogramowanie Antywirusowe z licencja na 17 stanowisk

Zamawiający wymaga dostawy 17 licencji oprogramowania antywirusowego na okres 12 miesięcy zgodnych z poniższą specyfikacją.

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	Administracja zdalna w chmurze	1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. 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. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. 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. 12. 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.
2.	Ochrona stacji roboczych – Windows	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. 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. 22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. 23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: • 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 e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

3.	Ochrona stacji roboczych - macOS	1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) lub nowszych. 2. Rozwiązanie musi wspierać architekturę Apple Silicon (ARM) 3. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim. 4. Pomoc w rozwiązaniu (help) musi być dostępna co najmniej w języku polskim oraz angielskim. 5. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 6. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 7. Rozwiązanie musi posiadać funkcjonalność, która w momencie wykrycia trybu pełnoekranowego ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań. 8. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. 9. Rozwiązanie musi posiadać możliwość zdalnego zarządzania z poziomu Administracji zdalnej. 10. Rozwiązanie musi umożliwiać 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).
4.	Ochrona stacji roboczych – Linux	1. Rozwiązanie musi wspierać systemy operacyjne Ubuntu Desktop, Red Hat Enterprise Linux oraz Linux Mint. 2. Rozwiązanie musi posiadać wsparcie dla dystrybucji 64-bitowych. 3. Pomoc (help) musi być dostępna co najmniej w języku polskim oraz angielskim. 4. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 5. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 6. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.

		7. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. 8. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". 9. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. 10. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
5.	Ochrona serwera	1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux 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. **Dodatkowe wymagania dla ochrony serwerów Windows:** 9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

		10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 13. 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. 14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. **Dodatkowe wymagania dla ochrony serwerów Linux:** 18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 21. 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 zawieszonego mikro-serwisu.

6.	Ochrona urządzeń mobilnych opartych o system Android	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: a.usunięcie zawartości urządzenia, b.przywrócenie urządzenie do ustawień fabrycznych, c.zablokowania urządzenia, d.uruchomienie sygnału dźwiękowego, e.lokalizację GPS. 6.Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7.Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: a.nazwę aplikacji, b.nazwę pakietu, c.kategorię sklepu Google Play, d.uprawnienia aplikacji, e.pochodzenie aplikacji z nieznanego źródła.

9. OPROGRAMOWANIE do wykonywania kopi zapasowych – 1 szt - Wymagany okres obowiązywania licencji – 12 m-cy

1	Ilość licencji	Backup dla 6 maszyn wirtualnych Windows oraz 3 serwerów fizycznych Windows Licencje bezterminowe z rocznym serwisem w cenie

2	Parametry techniczne	1. Pełne wsparcie dla systemów rodziny Microsoft Windows Server: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Storage Server 2012 R2 Essentials, Windows Server 2008 R2 Foundation, Windows Server 2008 Foundation z SP2 lub wyższy. 2. Pełne wsparcie dla systemów rodziny Windows Small Business Server: Windows Server 2012 R2 (Essentials, Foundation), Windows Server 2012 (Essentials, Foundation), Windows Small Business Server 2011, Windows Small Business Server 2008 (Standard i Premium), Windows Server 2008 R2 Foundation. 3. Pełne wsparcie dla środowisk wirtualnych: VMware Workstation, VMware ESX/ESXi, Microsoft Hyper-V, Microsoft Virtual PC, Microsoft Virtual Server, Oracle VirtualBox, Citrix XenServer, Linux KVM, ProxMox, Red Hat Enterprise Virtualization (RHEV), Stratos everRun. 4. Wsparcie dla 32 i 64-bitowych systemów Microsoft. 5. Wsparcie systemów plików: FAT16, FAT16X, FAT32, FAT32X, NTFS. 6. Wsparcie dla dysków z tablicą partycji MBR oraz GPT 7. Pełne wsparcie dla systemów Ubuntu 14.04, 16.04, 18.04, 20.04, CentOS 7, Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 8, Oracle Linux (wszystkie systemy 64-bitowe). 8. Wsparcie systemów plików: ext2, ext3, ext4, XFS. 9. Program i wsparcie techniczne dostępne w języku polskim 10. Wsparcie dla 32 i 64-bitowych systemów Microsoft: Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
3	Tworzenie kopii zapasowych (backupu)	1. Backup obejmuje kopie całego systemu operacyjnego wraz z konfiguracją oraz zainstalowanymi aplikacjami i plikami. 2. Program umożliwia skonfigurowanie różnych schematów wykonywania backupu: w trybie pełnym, backupy przyrostowe lub tryb mieszany. Harmonogram przyrostowy powinien umożliwiać backup z częstotliwością min. co 15 minut. 3. Istnieje możliwość wykonywania backupów pełnych i przyrostowych na dyski lokalne, dyski sieciowe, SAN, NAS, dyski USB, Firewire. 4. Program wykonuje kopie zapasowe (backupy) na poziomie sektorów czyli backup przyrostowy zawiera tylko zmienione sektory na dysku a nie np. całe pliki. 5. Program nie wymaga oddzielnego serwera zarządzającego backupem, a harmonogram zadań tworzenia backupów dla danej maszyny jest przechowywany bezpośrednio na tej maszynie. 6. Możliwe jest tworzenie kopii zapasowej w automatycznym trybie hot backupu (bez korzystania ze skryptów zamykających i uruchamiających bazy

		czy programy). Hot backup powinien pozwalać na backup systemu, aplikacji i baz danych takich MS SQL, MS Exchange, Active Directory, Share Point, Oracle od wersji 11g. 7. Do wykonywania kopii zapasowej wykorzystywana jest technologia Microsoft VSS oraz certyfikowany sterownik Microsoftu. 8. Program umożliwia wykonywanie kopii zapasowej dysku bez konieczności uruchamiania systemu operacyjnego za pomocą bootowalnej płyty lub pendrive'a z systemem i oprogramowaniem dostarczanym przez producenta rozwiązania backupowego. 9. Rozwiązanie pozwala na okresową weryfikacje, konsolidację oraz retencję łańcucha backupu przyrostowego z możliwością konfiguracji po jakim czasie mają się one wykonać. 10. Rozwiązanie musi umożliwiać tworzenie backupu przez łącze 3G i WiFi. 11. Podczas tworzenia kopii zapasowej program generuje plik sumy kontrolnej (md5) dla pliku backupu w celu kontroli plików backupu. 12. Program posiada narzędzie pozwalające na automatyczną weryfikację tworzonych plików backupu za pomocą okresowego uruchamiania backupowanego systemu operacyjnego w maszynie wirtualnej, oraz wysłanie zrzutu ekranu z tak uruchomionego systemu do administratora za pomocą wiadomości email. 13. Program umożliwia konwersje kopii zapasowej do plików dysków maszyn wirtualnych w formacie VHD, VMDK, VHDX. 14. Program umożliwia replikację wykonanych plików kopii zapasowych na dyski lokalnie, dyski sieciowe lub do lokalizacji zdalnych na serwer FTP.
4	Przywracanie z kopii zapasowych	1. Możliwość przywrócenia backupu całego obrazu dysku/partycji na takim samym sprzęcie, jak ten który był backupowany jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników do nowego sprzętu lub możliwość dodania sterowników przez użytkownika. Komputer powinien zostać uruchomiony z bootowalnej płyty CD lub pendrive'a, z którego bezpośrednio zostaje uruchomiony proces odzyskiwania obrazu dysku z backupu. 2. Program pozwala na dowolne odtwarzanie maszyn fizycznych na inną fizyczną lub do maszyny wirtualnej, oraz z maszyny wirtualnej do innej maszyny wirtualnej lub na fizyczną. 3. Bez względu na rozmiar backupu, program umożliwia automatyczne uruchomienie systemu z backupu jako maszyny wirtualnej w środowiskach VirtualBox, VMware vSphere lub Hyper-V bez konieczności wcześniejszej konwersji pliku backupu do postaci wirtualnej. 4. Program umożliwia zamontowanie pliku backupu jako dysku wirtualnego w trybie odczyt/zapis lub tylko do odczytu. Tak podłączony dysk logiczny

		umożliwia przeglądanie, wyszukiwanie i odzyskiwanie plików, folderów a także modyfikowanie zawartości. 5. Podczas przywracania obrazu dysku/partycji z kopii zapasowej, program umożliwia: uaktywnienie wybranej partycji, przywrócenia sektora MBR, przywrócenie sygnatur dysku, przywrócenie ukrytych ścieżek na dysku, dezaktywację licencji systemu Windows. 20. Program pozwala na zdefiniowanie procesu tworzenia kolejnych backupów przyrostowych, które w sposób automatyczny będą odtwarzane po określonym przez administratora czasie na innej maszynie fizycznej lub wirtualnej (VMDK, VHD, VHDX). Musi istnieć możliwość zdefiniowania opóźnienia z jakim kopie przyrostowe będą przenoszone na nowy wolumin w zakresie od 1 godziny do 30 dni.
5	Zdalne zarządzanie	1. Program musi umożliwiać pełną konfigurację i pełne zarządzanie zadaniami wykonywania kopii zapasowej na innych komputerach w sieci lokalnej, w zakresie identycznym jak z lokalnej konsoli administracyjnej. 2. Musi być dostępne narzędzie dające możliwość tworzenia zadań backupu za pomocą polityk dla grup stacji z poziomu konsoli webowej. 3. Konsola webowa musi umożliwiać instalację oraz aktualizację zdalną oprogramowania na punktach końcowych. 4. Konsola webowa musi umożliwiać podgląd dzienników zdarzeń na stacjach końcowych. 5. Program musi umożliwiać wysłanie powiadomień w postaci wiadomości e-mail gdy: zadanie backupu zakończyło się niepowodzeniem, po zakończeniu zadania tworzenia backupu, oraz podsumowanie aktywności dziennej, tygodniowej i miesięcznej. 6. Musi istnieć możliwość pobrania ze strony producenta konsoli zarządzającej w postaci pliku ISO.

10. Oprogramowanie do badania podatności systemów informatycznych wraz z licencją na 100 urządzeń - Wymagany okres obowiązywania licencji – 12 m-cy

L.P	**Parametr**	**Charakterystyka (wymagania minimalne)**
	Ogólne	1. Rozwiązanie typu vunlerability manager ma musi być dostępne w dwóch wersjach: lokalnej (on-premise) oraz chmurowej (SaaS). 2. Rozwiązanie w wersji chmurowej musi posiadać swoje centrum danych (data center) na terenie Unii Europejskiej. 3. Rozwiązanie w wersji lokalnej musi być udostępnione w postaci obrazu maszyny OVA, pozwalając na wdrożenie w środowisku wirtualnym VMware.

		4. Rozwiązanie musi oferować możliwość wdrożenia sond skanujących w postaci gotowych maszyn wirtualnych Scanner Appliance, które muszą być udostępnione w postaci obrazu maszyny OVA lub dysku VHDX. 5. Sonda skanująca Scanner Appliance musi wymagać rejestracji, w konsoli centralnej Security Center, przy użyciu wygenerowanego przez administratora sześcioznakowego tokena. 6. Konsola centralna Security Center musi posiadać możliwość uruchomienia dodatkowego uwierzytelnienia użytkowników, za pomocą 2FA wysyłanych w postaci wiadomości SMS. 7. Rozwiązanie musi posiadać możliwość integracji z systemami ticketowymi: Jira, TopDesk i ServiceNow. 8. Rozwiązanie musi posiadać możliwość wysyłania powiadomień do następujących systemów: Slack, Microsoft Teams i Webhooks. 9. Administrator w konsoli centralnej Security Center musi posiadać możliwość dodania dodatkowych użytkowników zarządzających. 10. Rozwiązanie musi posiadać możliwość dodania dodatkowych zestawów uprawnień (ról), które mogą być przypisane do użytkowników systemu. 11. Rozwiązanie musi posiadać możliwość zarządzania systemem przy użyciu interfejsu API.
	Zarządzanie zestawami urządzeń i aplikacji webowych	12. Rozwiązanie musi posiadać możliwość dodania ręcznego urządzeń i aplikacji webowych do skanowania. 13. Rozwiązanie musi posiadać możliwość importu listy urządzeń z pliku CSV. 14. Dodanie urządzeń musi odbywać się za pomocą podania pojedynczego adresu IP, zakresu adresów IP oraz adresu sieci wraz z maską. 15. Dodanie aplikacji webowej musi pozwalać na dodanie rodzaju autentykacji, białej i czarnej listy adresów URL oraz rozszerzeń do skanowania. 16. Przy dodawaniu urządzeń i aplikacji webowych administrator musi posiadać możliwość wyboru poziomu wpływu biznesowego z jednego z 4 poziomów: Neutral, Low, Medium i High. 17. Przy dodawaniu urządzeń i aplikacji webowych administrator musi posiadać możliwość wyboru znaczników (tagów). 18. Administrator musi posiadać możliwość dodania znaczników (tagów) statycznych wraz z odpowiednim kolorem.

		19. Administrator musi posiadać możliwość dodania znaczników (tagów) dynamicznych, które będą przypisywane do urządzeń po spełnieniu jednego z warunków: nazwy zestawu urządzeń, adresu IP z podanego zakresu, otwartych portów lub systemu operacyjnego.
	Skanowanie sieciowe	20. Rozwiązanie musi posiadać możliwość zapewnienia nieograniczonej liczby skanów i nieograniczonej liczby zaplanowanych skanów oraz skanów na żądanie. Powiadomienia powinny być również dostępne za pośrednictwem integracji e-mail, Slack i Webhook itp. 21. Rozwiązanie musi posiadać możliwość zapewnienia nieograniczonej liczby węzłów skanowania z nieograniczoną liczbą węzłów skanowania, które umożliwiają skanowanie różnych części sieci w tym samym czasie. 22. Rozwiązanie musi posiadać możliwość skanowania całego środowiska IT z segmentowanymi i geograficznie oddzielonymi sieciami. 23. Usługa skanowania sieci musi obsługiwać IPv6. 24. Rozwiązanie musi posiadać możliwość dodawania nowych profili skanowania sieciowego. 25. Administrator musi posiadać możliwość importu predefiniowanych przez producenta profili skanowania sieciowego. 26. Podczas tworzenia profilu skanowania, administrator musi posiadać możliwość wyboru trybu skanowania: Full, Basic lub Discovery. 27. Funkcja wykrywania urządzeń w profilu skanowania, musi pozwalać na wybór domyślnych portów, dodanie dodatkowych portów, wybór rodzaju połączenia TCP SYN lub TCP SYN ACK oraz możliwość wyłączenia lub włączenia wysłania ICMP PING. 28. Rozwiązanie musi posiadać możliwość uwzględnienia podatności o niskim prawdopodobieństwie wystąpienia w wynikach skanowania. 29. Rozwiązanie musi umożliwiać klientom wybór opcji "potencjalnie niebezpiecznych testów" i włączenia skanowania drukarek. 30. Rozwiązanie musi posiadać możliwość uwzględnienia martwych hostów w skanach. 31. Możliwość włączenia opcji - brutalnego wymuszania hasła - do ustawień skanowania.

		32. Profil skanowania sieciowego musi posiadać możliwość dodania uwierzytelniania na urządzeniu sieciowym, w oparciu o uwierzytelnianie Windows i/lub Linux. 33. Profil skanowania sieciowego musi posiadać możliwość wyboru intensywność skanowania. 34. Profil skanowanie sieciowego musi posiadać możliwość wyboru testów podatności, które będą przeprowadzone w trakcie skanowania. 35. Rozwiązanie musi posiadać co najmniej 80 tys. (w wersji lokalnej) i 130 tys. (w wersji chmurowej) testów podatności aktualizowanych na bieżąco z serwera producenta rozwiązania. 36. Podczas tworzenia zadania skanowania sieciowego, administrator musi posiadać możliwość wyboru sondy skanującej Scanner appliance zainstalowanej lokalnie, grupy sond lub sondy zewnętrznej hostowanej w chmurze producenta (tylko w wersji chmurowej). 37. Administrator musi posiadać możliwość uruchomienia zadania skanowania sieci jednorazowo lub z harmonogramem. 38. Rozwiązanie musi posiadać możliwość pobrania raportu CSV z modułu skanowania sieciowego w celu wyświetlenia listy zadań skanowania. 39. Urządzenia znalezione podczas zadania skanowania muszą zostać automatycznie dodane do listy urządzeń wraz z odpowiednimi znacznikami (tagami), przypisanymi na podstawie wykrytych portów usług oraz systemu operacyjnego. 40. Podatności wykryte podczas skanowania sieciowego muszą automatycznie być umieszczane w menedżerze podatności.
	Skanownie aplikacji webowych	41. Rozwiązanie musi posiadać możliwość dodawania nowych profili skanowania aplikacji webowych. 42. Administrator musi posiadać możliwość importu predefiniowanych przez producenta profili skanowania aplikacji webowych. 43. Rozwiązanie musi posiadać możliwość skanowania aplikacji internetowych (skanowanie stron internetowych). 44. Rozwiązanie musi posiadać możliwość zapewnienia nieograniczonej liczby skanów i nieograniczonej liczby zaplanowanych skanów oraz skanów na żądanie. Powiadomienia powinny być również dostępne za pośrednictwem integracji e-mail, Slack i Webhook itp.

		45. Rozwiązanie musi posiadać możliwość skanowania nieograniczonej liczby aplikacji internetowych. 46. Rozwiązanie musi posiadać możliwość zapewnienia konfigurowalnych ustawień skanowania, takich jak ustawienia indeksowania do metody formularza: Post i Get, Post, Get. 47. Podczas tworzenia zadania skanowania aplikacji webowych, administrator musi posiadać możliwość wyboru sondy skanującej Scanner appliance zainstalowanej lokalnie lub sondy zewnętrznej hostowanej w chmurze producenta (tylko w wersji chmurowej). 48. Podczas tworzenia profilu skanowania aplikacji webowych administrator musi posiadać możliwość włączenia i wyłączenia wykonania testów „łamania" haseł typu brute force. 49. Rozwiązanie musi posiadać możliwość wyboru intensywności skanowania wydajności (wstępnie ustawiona na niską, średnią i wysoką) przez system. Umożliwia również niestandardowe ustawienia żądań na sekundę. 50. Rozwiązanie musi posiadać możliwość włączenia pełnego zestawu kategorii wykrywania podatności, a także dostosowania kategorii wykrywania podatności do skanowania, a także listy wykluczeń. 51. Rozwiązanie musi posiadać możliwość wyboru opcji skanowania wrażliwych treści, numerów kart kredytowych i zezwalania na wprowadzanie niestandardowych treści. 52. Administrator musi posiadać możliwość uruchomienia zadania skanowania aplikacji webowej jednorazowo lub z harmonogramem. 53. Podatności wykryte podczas skanowania aplikacji webowych muszą automatycznie być umieszczane w menedżerze podatności.
	Skanowanie agentowe	54. Rozwiązanie musi posiadać możliwość instalacji na systemach Windows aplikacji agentowej, która będzie przesyłać do konsoli centralnej Security Center listę zainstalowanych aplikacji. 55. Systemu musi posiadać bazę podatności aplikacji zainstalowanych w systemach skanowanych przez aplikację agentową. 56. Wykryte przez aplikację agentową podatności muszą automatycznie być umieszczane w menedżerze podatności. 57. Pakiet instalacyjny aplikacji agentowej musi być udostępniony w postaci pliku .msi.

		58. Aktywacja aplikacji agentowej musi wymagać podania, wygenerowanego w konsoli centralnej Security Center, tokenu.
	Skanowanie usług chmurowych	59. Rozwiązanie musi posiadać możliwość wykrywania i raportowania błędnej konfiguracji usług chmurowych Amazon Web Services (AWS), Microsoft Azure oraz Google Cloud. 60. Rozwiązanie musi posiadać możliwość dodawania nowych profili skanowania usług chmurowych. 61. Administrator musi posiadać możliwość uruchomienia zadania skanowania usługi chmurowej jednorazowo lub z harmonogramem.
	Monitorowanie serwerów pocztowych i stron internetowych	62. Rozwiązanie musi posiadać mechanizm weryfikacji listowania na czarnych listach serwerów pocztowych i stron internetowych.
	Zarządzanie aktywami	63. Rozwiązanie musi posiadać możliwość wyświetlenia listy zeskanowanych zasobów: adres IP sieci i aplikacje internetowe z następującymi informacjami: a. Oznaczanie (lista grupowania) b. Nazwa zasobu c. Liczba wykrytych podatności w zabezpieczeniach d. Najwyższa wykryta podatność e. Krytyczność/istotność dla biznesu f. Informacje o systemie operacyjnym g. Data wprowadzenia utworzonych zasobów i ostatnio wykryty znacznik czasu 64. Rozwiązanie musi posiadać możliwość przeglądania informacji o aktywach, takich jak: a. Sieć: Stan podatności - Aktywne, Ignorowane i Wyłączone. b. Sieć : Status podatności - Nowa, Aktywna, Ponownie otwarta i Naprawiona c. Sieć: lista otwartych portów powiązanych z zasobem d. Sieć: Trend zasobu - według ważności, stanu. Możliwość wyświetlania według okresu i przedziału czasu. e. Aplikacja internetowa : Stan podatności - Aktywne, Ignorowane i Wyłączone. f. Aplikacja internetowa : Status podatności - Nowa, Aktywna, Ponownie otwarta i Naprawiona

		g. Aplikacja internetowa : Lista przeskanowanych i wykrytych map witryn h. Aplikacja webowa: Trend zasobu - według ważności, stanu. Możliwość wyświetlania według okresu i interwału. 65. Potrafi zapewnić możliwość edycji informacji o aktywach, takich jak: a. Sieć: Aby podać nazwę zasobu (jeśli nie jest dostępny DNS). b. Sieć: aby podać etykietę wpływu biznesowego c. Sieć: Aby podać kolumnę wejściową dla opisu zasobu d. Sieć: możliwość wybrania, czy zasób przechowuje jakiekolwiek dane osobowe RODO e. Aplikacja internetowa: Aby podać nazwę zasobu f. Aplikacja internetowa: Aby podać etykietę wpływu biznesowego g. Aplikacja internetowa: Aby zapewnić kolumnę wejściową dla opisu zasobu h. Aplikacja internetowa: Rozwiązanie musi posiadać możliwość wybrania, czy zasób przechowuje jakiekolwiek dane osobowe RODO i. Aplikacja internetowa: Rozwiązanie musi posiadać możliwość zapewnienia funkcji skanowania REST API j. Aplikacja internetowa: Może zapewnić zakres indeksowania, taki jak nazwa hosta adresu URL i podkatalog adresu URL. A także w stanie jawnie określić inne adresy URL k. Aplikacja webowa: Możliwość podawania nagłówków i plików cookie l. Aplikacja internetowa: może zapewnić uwierzytelnione skanowanie, takie jak HTTP Basic i HTTP Form m. Aplikacja internetowa: Może zapewnić elastyczność w utrzymywaniu listy wykluczających adresów URL, takich jak biała i czarna lista. n. Aplikacja internetowa: Rozwiązanie musi posiadać możliwość wyświetlenia listy zeskanowanych luk w zabezpieczeniach powiązanych z zasobami aplikacji internetowej. 66. Rozwiązanie musi potrafić zapewnić funkcje tworzenia i utrzymywania tagów (grup) statycznych i dynamicznych. 67. Rozwiązanie musi posiadać możliwość tworzenia ręcznego wprowadzania i importowania zasobów kategorii Network IP
	Moduł kampanii	68. Rozwiązanie musi posiadać możliwość utworzenia kampanii phishingowej i edukacyjnej dla **min. 20 użytkowników.**

	phishingowych i edukacyjnych	69. Administrator musi posiadać możliwość utworzenia własnych profili phishingowych lub importu predefiniowanych przez producenta. 70. Profile kampanii phishingowych utworzone przez producenta muszą być dostępne w języku polskim i angielskim. 71. Profil kampanii phishingowej powinien zawierać szablon wiadomości email lub wiadomości email i strony internetowej. 72. Rozwiązanie musi posiadać możliwość przypisania do profilu kampanii phishingowej kategorii domen, z których wysyłane będą wiadomości. 73. Rozwiązanie musi posiadać minimum 60 dostępnych domen przydzielonych do odpowiednich kategorii. 74. Kampanie phishingowe muszą posiadać możliwość wyboru czasu rozpoczęcia kampanii oraz czy wiadomości mają być wysyłane jednorazowo do wszystkich odbiorców, w grupach lub losowo w określonym zakresie czasu. 75. Platforma musi posiadać co najmniej 5 predefiniowanych szablonów kampanii: a. Polski: Wiadomości phishingowe - oszustwo związane z kontem e-mail b. Polski: Wiadomości phishingowe i strony internetowe - oszustwa związane z kontami e-mail c. Polski: Wiadomości phishingowe i strony internetowe - oszustwa związane z kartami kredytowymi d. Polski: Pobieranie plików - Office 365 e. Polski: Phishing - Office 365 76. Administrator musi posiadać możliwość przypisania do kampanii phishingowej, kampanii edukacyjnej przeprowadzanej poprzez wysłanie wiadomości email i/lub strony internetowej. 77. Administrator musi posiadać możliwość utworzenia własnych profili edukacyjnych lub importu predefiniowanych przez producenta. 78. Profile kampanii edukacyjnych utworzone przez producenta muszą być dostępne w języku polskim i angielskim. 79. Rozwiązanie musi posiadać możliwość wyboru treści wiadomości edukacyjnej w zależności od podjętej przez odbiorcę czynności: otwarcia wiadomości, odpowiedzi na wiadomość, kliknięcia w link oraz wypełnienia formularza na stronie phishingowej.

		80. Rozwiązanie musi posiadać możliwość stworzenia oraz wyboru treści prezentacji edukacyjnej w formie strony internetowej na której można zamieszczać treści edukacyjne w postaci tekstu, grafiki oraz wideo. 81. Rozwiązanie musi posiadać możliwość stworzenia oraz wyboru testu sprawdzającego wiedzę w formie strony internetowej na której można zamieszczać pytania i odpowiedzi w formie jednokrotnego i wielokrotnego wyboru. 82. Rozwiązanie musi posiadać możliwość anonimizacji danych odbiorców i podjętych przez nich czynności. 83. Rozwiązanie musi posiadać możliwość importu odbiorców wiadomości phishigowych z systemu Azure ActiveDirectory.
	Menedżer podatności i panel główny	84. Platforma zarządzania podatnościami musi być w stanie zapewnić funkcje pulpitu nawigacyjnego (i konfigurowalne) z następującymi widżetami: a. Wyniki skanowania podatności sieci według ważności (z opcjami wykresu: słupkowy i kołowy) b. Wyniki skanowania podatności aplikacji internetowych według ważności (z opcjami wykresu: słupkowy i kołowy) c. Otwarte zgłoszenia według ważności (z opcjami wykresu: słupkowy i kołowy) d. Top 10 wyników skanowania sieci (dostępna opcja ustawienia celu zasobu jako wszystkich lub wybranych adresów IP / tagów) e. 10 największych podatności w aplikacjach sieciowych (dostępna opcja ustawienia celu zasobu jako wszystkie lub wybrane aplikacje sieciowe/etykiety) f. Zgodność z OWASP (z opcjami wykresów : Słupkowy i kołowy oraz dostępną opcją ustawienia dla wszystkich lub wybranych aplikacji internetowych) g. Ostatnie skanowania h. Nadchodzące skanowania i. Ostatnie 10 raportów j. Liczba podatności w zabezpieczeniach w czasie (dostępna opcja ustawienia celu zasobu jako wszystkich lub wybranych aplikacji Ips / Web / tagów wraz z ustawieniem czasu, aby ustawić czas trwania i interwał) k. Ocena wyników kampanii phishingowych l. Ciągłe monitorowanie alertów (dostępna opcja ustawienia okresu na dzień/tydzień)

		85. Platforma zarządzania podatnościami musi mieć możliwość sortowania, grupowania i priorytetyzacji podatności a. Możliwość tworzenia wielu zakładek w celu filtrowania następujących kryteriów: b. Według stanu : Wszystkie, Nie ignorowane/wyłączone i ignorowane/wyłączone. c. Według typu: Host i aplikacja internetowa d. Według statusu : Nowy, Aktywny, Ponownie otwarty, Naprawiony e. Według ważności : Informacja, Niski, Średni, Wysoki, Krytyczny f. Według tagów (opcja uwzględnienia/wykluczenia tagu) g. Według pierwszego i ostatniego wykrycia h. Według kategorii: podatności w skanowaniu sieci i podatności w aplikacjach internetowych i. Możliwość filtrowania listy podatności według podatności lub aplikacji internetowych / hosta. j. Możliwość tworzenia raportów bezpośrednio z Menedżera podatności poprzez wybranie jednej lub więcej podatności. k. Możliwość dalszego administrowania / zarządzania listą luk w zabezpieczeniach za pomocą następujących funkcji: l. Co ignorować: Wyłącz tę podatność dla wszystkich hostów/aplikacji internetowych i Ignoruj tę podatność. m. Powód ignorowania : Fałszywie dodatni, Ryzyko zaakceptowane, Nieistotne n. Opcja ustawienia czasu wygaśnięcia dla ignorowanych podatności o. Możliwość tworzenia notatek do celów uwag i notatek, które pojawią się w raporcie po jego wygenerowaniu p. Możliwość tworzenia czatu konwersacyjnego do celów współpracy między użytkownikami q. Opcja wyświetlania następujących informacji na temat podatności - i. Wpływ ii. Rozwiązanie iii. Podsumowanie iv. Wgląd v. Wykrywanie vi. Odniesienie

		vii. Łatki viii. Możliwość utworzenia zgłoszenia bezpośrednio ze wskazanych luk w zabezpieczeniach ix. Środki zaradcze 86. Platforma jest w stanie zapewnić wbudowany system ticketowy dla procesu naprawczego. 87. Możliwość dostarczania informacji o zgłoszeniach, takich jak: a. Numerowanie ich w celu łatwego śledzenia i powiadamiania za pośrednictwem poczty elektronicznej. b. Możliwość podawania i aktualizowania statusu zgłoszenia, takiego jak : Otwarte, Zamknięte lub Rozwiązane c. Możliwość podania nazwy powiązanej podatności w zabezpieczeniach wraz z jej zasobami d. Możliwość podania wagi podatności w zabezpieczeniach zarejestrowanego zgłoszenia e. Możliwość przypisania do wyznaczonego właściciela i terminu płatności f. Możliwość tworzenia wielu zakładek do utrzymywania i zarządzania zgłoszeniami zgodnie z poniższymi zasadami: g. Status h. Typ zasobu i. Kategoria usługi j. Tagi k. Termin płatności l. Kategoria skanowania sieci i aplikacji internetowych m. Istotność n. System operacyjny o. Porty p. Właściciel q. Potrafi zapewnić proaktywną obsługę zgłoszeń opartą na zasadach 88. Rozwiązanie musi posiadać możliwość ciągłego monitorowania oraz szybkiego i łatwego ustawieniania profilu monitorowania zmian za pomocą powiadomień i alarmów. 89. W menedżerze podatności musi istnieć możliwość utworzenia własnego widoku podatności zawierającego odfiltrowane zgodnie z konfiguracją administratora danych. 90. Rozwiązanie musi posiadać możliwość zignorowania wykrytych podatności na określony czas.

	System raportujący	System raportujący musi zawierać następujące raporty: 91. Skanowanie sieci 92. Aplikacja sieciowa 93. Łatki 94. Środki zaradcze 95. Ocena phishingu e-mail 96. Porównanie (raport Delta) 97. Zgodność 98. Raporty zgodności: Musi być w stanie wygenerować następujący typ zgodności: a. Ustawa Sarbanes-Oxley b. Ustawa o przenośności i rozliczalności ubezpieczeń zdrowotnych c. OWASP Top 10 (2017) d. Ustawa o ochronie danych osobowych e. ISO / IEC 27001 f. Ogólne rozporządzenie o ochronie danych g. Bezpieczeństwo sieci i informacji h. PCI DSS 99. System powinien mieć możliwość dostarczania nowych niestandardowych raportów zgodności, które mogą być zalecane przez rząd, gdy ma to zastosowanie. 100. Rozwiązanie musi posiadać możliwość tworzenia i dostosowywania szablonów raportów sieciowych z następującymi opcjami: a. Raport oparty na określonym czasie skanowania b. Raport oparty na wszystkich bieżących informacjach o podatnościach c. Raport trendów z historią podatności d. Zawartość raportu : Szczegóły raportu, przegląd podatności, podsumowanie podatności, lista podatności (według podatności i hosta) z opcjami wglądu, podsumowania, wykrywania, odniesień i ograniczenia tekstu do 500 znaków. e. Sposób prezentacji raportu: Podatności według ważności w czasie, Podatności według statusu, Podatności według ważności, 5 najbardziej narażonych kategorii f. Filtrowanie: Selektywne raportowanie podatności (pełne i niestandardowe) i wykluczenia, Uwzględnione systemy operacyjne, Filtry zasobów, Filtry podatności

		101. Potrafi utworzyć i dostosować szablon raportu aplikacji internetowej z następującymi opcjami: 102. Raport oparty na określonym czasie skanowania 103. Raport oparty na wszystkich bieżących informacjach o podatnościach 104. Zawartość raportu : Szczegóły raportu, Przegląd podatności, Podsumowanie podatności, Lista podatności (według podatności i hosta) z opcjami Wglądu, Podsumowania, Wykrywania, Odniesień i Ograniczenia tekstu do 500 znaków. 105. Filtrowanie: Selektywne raportowanie podatności (pełne i niestandardowe) i wykluczenia, Uwzględnione systemy operacyjne, Filtry zasobów, Filtry podatności 106. Możliwość tworzenia "raportów skróconych" wysyłanych w sposób podsumowujący. Częstotliwość raportów można ustawić na: tygodniowe raporty skrócone i miesięczne raporty skrócone. Raporty są dostarczane kanałem e-mail.