Cyberbezpieczne Wodociągi

Załącznik Nr 2 do Zapytania

Opis przedmiotu zamówienia (OPZ)

Przedmiot zamówienia obejmuje dostawę sprzętu i oprogramowania informatycznego oraz usług opisanych szczegółowo w poniższych rozdziałach, wraz z ich wdrożeniem zgodnie z zakresem wdrożenia określonym w rozdziale końcowym.

Gmina Dołhobyczów - Gminny Zakład Usług Komunalnych w Dołhobyczowie
ul. Usługowa 5, 22-540 Dołhobyczów

(znak sprawy: GZUK.26.3.2026)

1. **Serwer – 1 sztuka**

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 2U • 12 slotów na dyski 3.5” • 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.
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora • Obsługa procesorów 80 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinny znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do 1.5TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	• Zainstalowany jeden procesor min. 16-to rdzeniowy, klasy x86 dedykowany do pracy z zaoferowanym serwerem dający w teście Passmark dostępnym na stronie https://www.cpubenchmark.net/wynik nie mniejszy niż 46800
RAM	• 128GB RAM w modułach DDR5 RDIMM 6400MT/s,

Kontroler	Urządzenie powinno wykorzystywać interfejs hosta **PCIe Gen4 x16**. Kontroler powinien technologicznie zapewniać obsługę do **240 dysków SAS/SATA** oraz do **24 dysków NVMe**. Powinien on wspierać przepustowości danych do **22,5 Gb/s dla standardu SAS 4.0** (24 Gbps), 12 Gb/s dla SAS 3.0 oraz 6 Gb/s dla SATA 3.0, a także do **16 GT/s dla napędów NVMe Gen4**. Powinien realizować sprzętową obsługę poziomów **RAID 0, 1, 5, 6, 10, 50 i 60** Kontroler powinien być wyposażony w **8 GB dedykowanej pamięci cache DDR4 (3200 MT/s)**. Ochronę danych w pamięci podręcznej powinien zapewniać system podtrzymania zasilania oparty na **module energii (bateria lub superkondensator)** współpracujący z **nieulotną pamięcią flash (NVC)**, co powinno umożliwiać zachowanie zawartości cache w przypadku awarii zasilania. Bezpieczeństwo operacyjne powinien gwarantować sprzętowy mechanizm **Root of Trust (RoT)**, uwierzytelniający firmware przed uruchomieniem, oraz protokół **SPDM** do weryfikacji autentyczności urządzenia. Urządzenie powinno zapewniać pełną zgodność z **UEFI Secure Boot** przy jednoczesnym braku wsparcia dla trybu Legacy BIOS. Kontroler powinien wspierać obsługę dysków samoszyfrujących (**SED**) zgodnych ze standardami TCG Enterprise i Opal, oferując lokalne oraz zewnętrzne zarządzanie kluczami bezpieczeństwa. Funkcjonalność kontrolera powinna obejmować **dynamiczne rozszerzanie pojemności online (OCE)**, monitorowanie parametrów **SMART**, mechanizm **Patrol Read** do skanowania integralności nośników oraz zaawansowaną diagnostykę typu

	Snapdump. Zarządzanie urządzeniem powinno odbywać się poprzez interfejsy **CLI** oraz narzędzia konfiguracyjne zintegrowane z **BIOS**, umożliwiając aktualizację firmware w trybie online.
Dyski twarde	• Zainstalowane: ○ 4x dyski 960GB SSD Hot-Plug
Gniazda PCI	• dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	• Wbudowane 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT porty nie mogą być osiągnięte poprzez karty w slotach PCIe • Dodatkowa karta sieciowa PCI Express Gen 4.0 x16 z czterami portami SFP28, obsługa prędkości 10/25 GbE na każdym porcie (line-rate, full-duplex)
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	• Redundantne, Hot-Plug min. 1100W klasy Titanium
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych z ramieniem na kable
Bezpieczeństwo	• Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • 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 V3 • 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). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego spełnienie powyższych zaleceń.
Karta Zarządzania	Karta zarządzania powinna posiadać następujące cechy i możliwości: • Zdalne zarządzanie bezagentowe: Możliwość pełnego, bezagentowego monitorowania stanu zdrowia kluczowych podzespołów, takich jak procesory, pamięć RAM, zasilacze oraz systemy chłodzenia, bez konieczności instalowania dodatkowego oprogramowania w systemie operacyjnym hosta. • Sprzętowy mechanizm zaufania (Silicon Root of Trust): Zintegrowany w krzemie mechanizm zapewniający bezpieczny rozruch (Secure Boot), weryfikację integralności oprogramowania układowego (firmware) oraz sprzętowe poświadczanie autentyczności urządzenia. • Dedykowany port serwisowy nowej generacji: Dostęp do funkcji bezpośredniego zarządzania oraz diagnostyki poprzez dedykowane złącze USB typu C (Dual-Mode) umieszczone na przednim panelu serwera, działające w trybie dedykowanym dla kontrolera. • Nowoczesne i ustandaryzowane interfejsy zarządzające: Dostęp do graficznego interfejsu użytkownika opartego na standardzie HTML5 (bez potrzeby stosowania wtyczek

	Java/ActiveX) oraz wsparcie dla standardów automatyzacji Redfish API i wiersza poleceń RACADM. • Zapewnienie bezpieczeństwa dostępu: Dostarczenie każdego urządzenia z unikalnym, fabrycznie zdefiniowanym hasłem domyślnym, co eliminuje ryzyka związane ze stosowaniem generycznych danych logowania w infrastrukturze. • Mechanizm bezpiecznej utylizacji danych (Secure Erase): Funkcja trwałego i bezpiecznego usuwania zawartości z lokalnych nośników danych (HDD, SSD, NVMe) bezpośrednio z poziomu kontrolera zarządzającego, niezbędna przy wycofywaniu serwera z eksploatacji. • Rozbudowane dzienniki zdarzeń i inwentaryzacja: Prowadzenie szczegółowych dzienników zdarzeń systemowych (SEL) oraz logu cyklu życia (Lifecycle Log), a także automatyczne zbieranie i przechowywanie pełnej inwentaryzacji sprzętowej i programowej serwera. • Zaawansowana diagnostyka awarii (Crash Screen Capture): Możliwość automatycznego wykonywania i zapisywania statycznego zrzutu ekranu (obrazu JPEG) w momencie wystąpienia krytycznej awarii systemu operacyjnego hosta w celu ułatwienia diagnostyki. • Eksport profili konfiguracyjnych (SCP): Możliwość wyeksportowania pełnej konfiguracji serwera, w tym ustawień BIOS, kontrolera zarządzającego oraz kontrolerów RAID, do otwartego formatu danych XML lub JSON w celach archiwalnych i kopii zapasowej. • Kompleksowa łączność sieciowa: Pełne wsparcie dla protokołów IPv4 oraz IPv6, obsługa DHCP, tagowania VLAN, wizualizacji połączeń sieciowych (LLDP Connection View) oraz automatycznej rejestracji nazwy kontrolera w systemie DNS
Oprogramowanie do zarządzania	• Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: o wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; o - możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;

	○ - wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH; ○ - możliwość oskryptowywania procesu wykrywania urządzeń; ○ - możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram; ○ - szczegółowy opis wykrytych systemów oraz ich komponentów; ○ - możliwość eksportu raportu do CSV, HTML, XLS; ○ - grupowanie urządzeń w oparciu o kryteria użytkownika; ○ - automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń; ○ - 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; ○ - aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania); ○ - możliwość instalacji sterowników i 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 seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów

	PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformami wirtualizacji. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.

	○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów

	▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware o możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty o Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, o Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji o Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo

	○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 (lub równoważną) • Serwer musi posiadać deklaracje CE (lub równoważne). • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu. Duże części plastikowe nie mogą zawierać farb ani powłok, które uniemożliwiają ich

	ponowne użycie lub poddanie recyklingowi. Wszystkie podzespoły elektroniczne oraz komponenty zawierające składniki niebezpieczne muszą być bezpiecznie i łatwo identyfikowalne oraz możliwe do demontażu. Usunięcie tych materiałów i komponentów musi odbywać się zgodnie z przepisami krajowymi wdrażającymi Dyrektywę Parlamentu Europejskiego i Rady 2012/19/UE z dnia 4 lipca 2012 r. w sprawie zużytego sprzętu elektrycznego i elektronicznego (WEEE). Produkty muszą składać się w co najmniej 65% z części i komponentów nadających się do ponownego użycia lub recyklingu. Części z tworzyw sztucznych o masie powyżej 25 gramów mogą zawierać wyłącznie śladowe ilości środków zmniejszających palność (retardantów), które są sklasyfikowane jako stwarzające zagrożenie zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 1272/2008 (CLP). • Potwierdzenie spełnienia wymogów (Kryterium i Równoważność): ○ Zamawiający uzna wymóg za spełniony, jeżeli wykonawca wykaże, że oferowany produkt posiada certyfikat EPEAT na poziomie co najmniej Silver (Srebrny) (lub wyższym, np. zarejestrowany w rejestrze EPEAT 2.0). Dowodem może być wydruk ze strony internetowej oficjalnego rejestru EPEAT potwierdzający ten status. ○ Dopuszczenie rozwiązań równoważnych: Zamawiający dopuszcza wszelkie inne równoważne środki dowodowe. Jeśli oferowany produkt nie posiada certyfikatu EPEAT, wykonawca zobowiązany jest złożyć wraz z ofertą inne dokumenty jednoznacznie potwierdzające spełnienie wszystkich cech środowiskowych opisanych w pkt 1–4 (np. deklarację producenta, raporty z niezależnych badań laboratoryjnych lub certyfikaty innych równoważnych systemów oznakowania ekologicznego typu I wg ISO 14024). **- Wykonawca złoży dokument potwierdzający spełnianie ww. wymogu – przy odbiorze końcowym przedmiotu umowy.** • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025 (jeśli dotyczy).

Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub w języku obcym przetłumaczonym na język polski. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
System operacyjny	• Windows Server 2025 Standard
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii **na okres min. 3 lat.** • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 (całodobowo) następującymi kanałami: telefonicznie oraz przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. • Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:

	○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • **Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych (lub równoważne) oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć przy protokole odbioru.**

2. System operacyjny i licencje

Wymagania ogólne

Oferowane rozwiązanie musi:

- być przeznaczone do pracy w środowisku serwerowym;
- obsługiwać architekturę 64-bit;
- umożliwiać instalację na serwerach fizycznych;
- umożliwiać instalację oraz pracę jako system operacyjny maszyny wirtualnej;
- zapewniać obsługę wieloprocesorowych platform serwerowych;
- umożliwiać wykorzystanie wielu rdzeni procesora;
- zapewniać stabilną pracę w środowisku produkcyjnym 24/7;
- posiadać mechanizmy zarządzania użytkownikami, grupami oraz uprawnieniami;
- umożliwiać centralne zarządzanie konfiguracją i politykami bezpieczeństwa;
- umożliwiać zdalne zarządzanie systemem.

Usługi katalogowe i zarządzanie użytkownikami

System musi umożliwiać:

- integrację z usługą katalogową;
- tworzenie i zarządzanie użytkownikami oraz grupami;
- centralne zarządzanie uprawnieniami;
- stosowanie centralnych zasad bezpieczeństwa;
- zarządzanie komputerami i serwerami przyłączonymi do domeny;
- realizację mechanizmów uwierzytelniania użytkowników;
- stosowanie polityk bezpieczeństwa dla użytkowników i urządzeń.

Usługi sieciowe

System musi zapewniać możliwość realizacji co najmniej następujących funkcji:

- obsługa protokołów IPv4 i IPv6;
- obsługa usług DNS;
- obsługa usług DHCP;
- obsługa usług plikowych;
- obsługa udziałów sieciowych;
- zarządzanie dostępem do zasobów sieciowych;
- obsługa mechanizmów kontroli dostępu;
- możliwość integracji z istniejącą infrastrukturą sieciową Zamawiającego.

Wirtualizacja

System musi:

- umożliwiać uruchamianie maszyn wirtualnych;
- umożliwiać tworzenie i zarządzanie środowiskami wirtualnymi;
- wspierać przydzielanie zasobów CPU, pamięci RAM oraz przestrzeni dyskowej maszynom wirtualnym;
- umożliwiać uruchamianie wielu instancji systemów operacyjnych na jednym serwerze fizycznym;
- umożliwiać zarządzanie maszynami wirtualnymi lokalnie oraz zdalnie.

Bezpieczeństwo

Oferowany system musi zapewniać mechanizmy bezpieczeństwa obejmujące co najmniej:

- kontrolę dostępu do zasobów;
- zarządzanie uprawnieniami użytkowników;
- mechanizmy uwierzytelniania;
- mechanizmy ochrony danych;
- bezpieczny proces uruchamiania systemu;
- ochronę przed nieautoryzowanym dostępem;
- możliwość stosowania polityk bezpieczeństwa;
- możliwość instalowania aktualizacji bezpieczeństwa;
- rejestrowanie zdarzeń systemowych i bezpieczeństwa.

Zarządzanie i administracja

System musi umożliwiać:

- lokalne zarządzanie systemem;
- zdalne zarządzanie systemem;
- zarządzanie za pomocą interfejsu graficznego;
- zarządzanie za pomocą interfejsu wiersza poleceń;
- automatyzację zadań administracyjnych za pomocą skryptów;
- monitorowanie zasobów systemowych;
- przeglądanie dzienników zdarzeń;
- konfigurację usług systemowych;
- zarządzanie aktualizacjami.

System plików i przechowywanie danych

System musi zapewniać:

- obsługę systemów plików stosowanych w środowiskach serwerowych;
- obsługę dużych wolumenów danych;
- obsługę udziałów sieciowych;
- mechanizmy kontroli dostępu do plików i katalogów;
- możliwość stosowania uprawnień użytkowników i grup;
- możliwość integracji z rozwiązaniami backupowymi.

Licencjonowanie

Licencjonowanie musi być oparte na liczbie fizycznych rdzeni procesorów serwera, zgodnie z zasadami licencjonowania producenta.

Wymagana liczba licencji musi obejmować wszystkie fizyczne rdzenie procesorów serwera, z zachowaniem minimalnej liczby licencji wymaganej przez producenta.

Licencja musi umożliwiać uruchomienie co najmniej dwóch środowisk systemu operacyjnego na odpowiednio licencjonowanym serwerze fizycznym.

Możliwość uruchamiania dodatkowych środowisk systemu operacyjnego musi być zapewniona poprzez odpowiednie zwiększenie liczby przypisanych licencji.

Licencje dostępowe

Oferowane rozwiązanie musi zapewniać możliwość legalnego dostępu użytkowników lub urządzeń do usług serwera.

Wykonawca musi uwzględnić w ofercie odpowiednią liczbę licencji dostępowych dla użytkowników lub urządzeń, zgodnie z wymaganiami Zamawiającego.

Jeżeli wykorzystywane będą dodatkowe usługi wymagające odrębnych licencji dostępowych, Wykonawca musi uwzględnić je w ofercie.

Aktualizacje

System musi zapewniać możliwość:

- pobierania aktualizacji systemowych;
- pobierania aktualizacji bezpieczeństwa;
- instalowania poprawek;
- centralnego zarządzania procesem aktualizacji;
- utrzymywania systemu w aktualnym stanie bezpieczeństwa.

Kompatybilność

Oferowane rozwiązanie musi być kompatybilne z:

- serwerami x86-64;
- środowiskami wirtualizacyjnymi;
- urządzeniami sieciowymi;
- systemami backupowymi;
- rozwiązaniami antywirusowymi i bezpieczeństwa;
- usługami katalogowymi;
- istniejącą infrastrukturą IT Zamawiającego.

Wymagania dotyczące dostawy

Wykonawca zobowiązany jest dostarczyć:

- wymagane licencje;
- dokument potwierdzający legalność pochodzenia licencji;
- informacje niezbędne do aktywacji;
- dokumentację licencyjną;
- informacje dotyczące sposobu licencjonowania i liczby dostarczonych licencji.

Licencje muszą pochodzić z legalnego kanału dystrybucji producenta.

Minimalne wymagania ilościowe

Lp.	Element	Wymaganie
1	Licencja serwerowego systemu operacyjnego	1 komplet
2	Licencjonowanie rdzeni procesora	Wszystkie fizyczne rdzenie
3	Minimalna liczba licencjonowanych rdzeni	Zgodnie z wymaganiami producenta
4	Środowiska systemu operacyjnego	Min. 2
5	Licencje dostępowe	Zgodnie z liczbą użytkowników/urządzeń

Odbiór

Przedmiot zamówienia zostanie uznany za wykonany po:

- dostarczeniu wymaganych licencji;
- przekazaniu dokumentów potwierdzających ich legalność;
- potwierdzeniu możliwości aktywacji;
- potwierdzeniu zgodności liczby licencji z zamówieniem;
- przekazaniu wymaganej dokumentacji.

Gwarancja legalności licencji

Wykonawca gwarantuje, że dostarczone licencje są legalne, pochodzą z autoryzowanego lub legalnego kanału dystrybucji oraz uprawniają Zamawiającego do korzystania z oprogramowania zgodnie z warunkami licencyjnymi producenta.

Wykonawca ponosi odpowiedzialność za wszelkie roszczenia wynikające z dostarczenia licencji nielegalnych, nieautoryzowanych lub niezgodnych z wymaganiami producenta.

2. NAS – 2 serwery

Lp.	2 komplety serwer NAS + dyski o minimalnych poniższych parametrach:	
1.	Procesor	Dwurdzeniowy procesor AMD Ryzen R1600 2,6 GHz
2.	Obudowa	Rack 1U o wymiarach max. 45 × 479 × 328 mm; szyny teleskopowe do instalacji w szafie RACK
3.	Pamięć RAM	Pamięć 2 GB DDR4 ECC SODIMM

4.	Ilość obsługiwanych dysków	4 dysków 3,5" lub 2,5" SATA HDD/SSD
5.	Interfejsy sieciowe	2 porty 1GbE RJ-45
6.	Porty	1 port USB 3.2 1. Generacji 1x PCIe Gen3x 2
7.	Wskaźniki LED	Zasilanie, alert, status, LAN, HDD1-4
8.	Obsługa RAID	Synology Hybrid RAID (SHR), Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6 i RAID 10
9.	Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
10.	Licencja na Kamery IP	W zestawie dwie licencje na jedną kamerę z możliwością rozszerzenia do 40.
11.	Protokoły	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP i VPN (PPTP, OpenVPN™, L2TP)

12.	Usługi	Wsparcie dla High Availability Serwer VPN Stacja monitoringu Windows ACL Integracja z Windows ADS Firewall z kontrolą ruchu Serwer WWW Serwer plików Manager plików przez WWW Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie Antyvirus Klient VPN Usługa DDNS Oprogramownie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji VMware

13.	Obsługa migawek	• Maksymalna liczba migawek na foldery współdzielone: 128 • Maksymalna liczba migawek systemu: 256
14.	Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów,
15.	Język GUI	Polski
16.	Gwarancja i serwis	**Minimum 3 lata gwarancji**
17.	Waga	Max. 5 KG
18.	Certyfikaty	CE
19.	System plików	Wewnętrzny: Btrfs, ext4 Zewnętrzny: Btrfs, ext4, ext3, FAT32, NTFS, HFS+, exFAT
20.	Liczba wolumenów	Minimum 64
21.	Liczba iSCSI Targetów	Minimum 2

22.	Liczba iSCSI LUN	Minimum 2
23.	Liczba kont użytkowników	Minimum 512
24.	Liczba grup	Minimum 256
25.	Liczba udziałów	Minimum 128
26.	Chłodzenie	FAN x 3 40 x 40 mm
27.	Dyski	2 dyski HDD 3,5” o parametrach: - pojemność minimum 4TB - minimum 5400 RPM - minimum 256MB Cache - MTBF 1 mil. Godzin - Pobór mocy w trybie pracy max. 4.8W - Pobór mocy w trybie bezczynności max. 3.96W - Usługa odzyskiwania danych z dysków wykonywana przez producenta lub wykonawcę

3. Przełącznik dostępowy (sieciowy zarządzalny) – 2 sztuki

Gigabitowy przełącznik dostępowy

Porty przełącznika: minimum 24x 10/100/1000Base-T RJ45 oraz minimum 6x 1/10GBase-X SFP+
Port konsolowy: RJ45 (RS-232)
Port zarządzania: RJ45 (10/100Base-T RJ45)
Port USB: minimum 1 port co najmniej w standardzie 2.0
Szybkość przełączania: minimum 168Gb/s
Przepustowość: minimum 125Mp/s (dla pakietów 64Kb)
Bufor pakietów: minimum 2MB
Ramki Jumbo: minimum 12k
Tablica adresów MAC: minimum 32k
Adresy MAC – Multicast: minimum 2k
Tablica ACL: minimum 3k
Tablica VLAN: minimum 4k
Tablica routingu: minimum 1k dla IPv4 z możliwością wykorzystania IPv6. Dopuszcza się rozwiązania współdzielące tablicę routingu dla IPv4 oraz IPv6 w maksymalnej proporcji 4:1.
Taktowanie procesora: minimum 1G
Pamięć Flash: minimum 32MB + 128MB NAND
Pamięć RAM: minimum 1G
Temperatura pracy: zakres minimum 0°C - 50°C
Wilgotność względna: zakres minimum 10% - 90% (bez kondensacji)
Zasilanie: zabudowany zasilacz 230V AC
Pobór mocy: maksymalnie 40W
Zabezpieczenie przeciwprzepięciowe: minimum 6kV
Wymiary: maksymalna: szerokość 440 mm, wysokość 44mm , głębokość 380mm
Certyfikaty bezpieczeństwa: CE, RoHS

Algorytm pracy: Store and Forward
Obsługa VLAN: Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ
DHCP: IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server
Drzewo rozpinające: IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding, Fast Link, Loopback Detection,
Protekcja ringowa: ITU-T G.8032 – recovery time < 50ms,
Protokoły routingu: Static Routing, RIPv1/v2, RIPng, OSPFv2/v3, BGP4, BGP4+, OSPF multiple process, LPM Routing, Policy-based Routing (PBR) IPv4/IPv6, VRRP, IPv6 VRRPv3, URPF IPv4/IPv6,

ECMP, BFD, Static Multicast Route, Multicast Receive Control, Illegal Multicast Source Detect, GRE Tunnel, ISIS
Agregacja linków: IEEE 802.3ad (LACP), 128 groups per device / 8 ports per group, load balance
Bezpieczeństwo: Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,
Multicast: IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, PIM-SM, PIM-DM, PIM-SSM, IGMP authentication
QoS: 8 queques per port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI Mark/Remark, IEEE 802.1p, Queuing Method: SP, WRR, SP+WRR; DNS Client, DNS Relay
Lista Kontroli Dostępu: IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Precedence, Vlan Tag/Untag, Rules can be configured to port and VLAN
Diagnostyka: sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route, Dying GASP
Zarządzanie: TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (4 devices in one stack) – hardware stacking
Oprogramowanie oraz wsparcie techniczne: oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług

Gwarancja: minimum 60 miesięcy.

4. Zasilacz awaryjny UPS 3000VA – 2 szt.

Lp.	Nazwa elementu, parametru lub cechy	Opis minimalnych wymagań
1	Moc pozorna	3000 VA

2	Moc rzeczywista	3000 W
3	Architektura UPSa	line-interactive
4	Liczba, typ gniazd wyj. z podtrzymaniem zasilania i ochroną przepięciową	8 x IEC320 C13 (10A) + 2 x C19 (16A)
5	Segmentacja gniazd odbiorów	Gniazda odbiorcze muszą zawierać co najmniej 2 grupy 2 x IEC C13, których sterowanie odbywać się powinno za pomocą oprogramowania. Każdy segment musi umożliwiać pomiar zużycia energii.
6	Kształt napięcia wyjściowego przy pracy bateryjnej	Sinusoidalny
7	Typ gniazda wejściowego	IEC320 C14 (10A)
8	Czas podtrzymania przy 100%	20 minut

	obciążeniu (3000W)	
9	Wysokość w szafie (UPS + moduł bateryjny)	4U
10	Typ obudowy	Uniwersalna Tower / Rack
11	Sprawność w trybie normalnym	> 96%
12	Zakres napięcia wejściowego w trybie podstawowym	160V - 294 V (regulowane do 150V - 294V)
13	Zakres częstotliwości wejściowej bez użycia baterii	47 do 70 Hz (sieć 50 Hz)
14	Poziom hałasu w trybie sieciowym	< 40 dBA

15	Zakres zmian napięcia wyjściowego	maksymalnie -10/+6% wartości nominalnej
16	Baterie wymieniane przez użytkownika "na gorąco"	Tak
17	Porty komunikacji	port szeregowy RS232, port USB, gniazdo rozszerzenia opcji komunikacji do instalacji karty SNMP/Web z możliwością monitorowania środowiska, port zdalnego wyłączania i włączania UPSa, mini złącze dla wyjściowego styku przekaźnikowego, styki bezpotencjałowe (3 wyjścia)
18	Pasek LED informujący o stanie UPS	Tak
19	Panel komunikacyjny	Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa) ze wskazaniami chwilowego poziomu obciążenia i poziomu naładowania baterii, z możliwością sterowania poszczególnymi segmentami odbiorów oraz pomiarem sprawności i zużycia energii przez odbiory (w kWh)

20	Alarmy dźwiękowe	• praca z baterii
		• awaria UPSa
		• przeciążenie UPSa
		• znaczne wyczerpanie baterii
21	Wyposażenie standardowe	• kabel zasilający
		• kable sygnałowe USB i RS232
		• kabel odbiorów 1.8m IEC320 C13/C14 - 2 szt.
		• system blokowania kabli - 2 szt.
		• zestaw montażowy do szafy 19"
		• podstawki do montażu tower

22	Wyposażenie dodatkowe	• karta SNMP
23	Karta SNMP	• cyberbezpieczeństwo (szyfry TLS, MQTT)
		• certyfikaty CA i PKl
		• prędkość gigabit'owa (half-duplex, full-duplex)
		• różne poziomy nadawania dostępu do konta administratora lub użytkownika
24	Oprogramowanie umożliwiające	• monitorowanie UPS oraz bezpieczne zamykanie urządzeń pracujących z systemami operacyjnymi Windows, Linux (RedHat, Fedora, (open) SUSE, Debian, Ubuntu), Unix (HP-UX, IBM Aix, Oracle (Sun) Solaris)
		• podłączenie UPS zarówno za pomocą interfejsu USB lub RS-232, jak i przez sieć

		• tworzenie scenariuszy wysyłania powiadomień email oraz uruchamiania własnych skryptów przy wystąpieniu wybranych zdarzeń
		• tworzenie indywidualnych kont użytkowników z co najmniej dwoma poziomami dostępu do wyboru
		• zdalny dostęp do swojego interfejsu graficznego po lokalnej sieci
		• wybór polskiej wersji językowej
25	System zarządzania pracą baterii	System nieciągłego ładowania baterii. **Do odbioru końcowego** dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
26	Możliwość wydłużenia czasu potrzymania	Tak. Do min. 80 minut dla obciążenia 2500W poprzez dołączenie baterii zewnętrznych - automatyczna detekcja zewnętrznych jednostek bateryjnych.

27	Certyfikaty	Deklaracja zgodności oraz certyfikat ISO 9001 producenta, certyfikat Energy Star (lub równoważny)
28	**Gwarancja co najmniej**	**3 lata**
29	Inne	Wszystkie elementy mają być nowe, nieużywane i wyprodukowane przez producenta UPS-a**. Do odbioru końcowego_należy załączyć oświadczenie producenta potwierdzające ten fakt i o pochodzeniu sprzętu z oficjalnego kanału dystrybucji na rynek Polski lub Unii Europejskiej**

6. System PAM (Privileged Access Management)

Wymagania funkcjonalne dla system

- Zapewnienie wysokiego poziomu bezpieczeństwa danych i poufności informacji
- Wsparcie dla szyfrowania danych w transmisji i przechowywaniu haseł i kluczy
- Elastyczność w zakresie skalowania infrastruktury w celu obsługi zwiększonego obciążenia
- System musi posiadać Mechanizmy failover i redundancji, aby zapewnić ciągłość działania w przypadku awarii serwera lub innego komponentu
- System PAM musi posiadać przyjazny interfejs graficzny (GUI) umożliwiający łatwe zarządzanie kontami uprzywilejowanymi i monitorowanie działań użytkowników.
- Integracja z technologią ZTNA (Zero Trust Network Access) oraz możliwość działania jako punkt wymuszania dla ZTNA
- Musi istnieć możliwość sprawdzania silnikiem antywirusowym przesyłanych podczas sesji plików. Kontrola musi być realizowana co najmniej dla transferu plików poprzez web (Web SFTP, Web SAMBA) oraz SCP.
- Automatyczne blokowanie niebezpiecznych poleceń za pomocą profilu filtrowania SSH. System musi monitorować komendy wydawane przez operatora sesji.
- System PAM powinien być dostarczony jako urządzenie na utwardzonym przez jednego producenta systemie operacyjnym w formie gotowego i pełnego rozwiązania
- Rozwiązanie musi być dostępne w formie zarówno urządzeń wirtualnych (*virtual appliance*), jak i sprzętowych. Dla wirtualizacji musi być wspierane co najmniej dwóch różnych hypervisorów wiodących producentów.
- Działanie PAM musi pozwalać na obsługę połączeń bezpośrednich jak i proxy.
- Możliwość obsługi niestandardowych protokołów chociażby poprzez dedykowane wyzwalacze (*custom application launcher*)
- Możliwość ostrzegania użytkowników o nagrywaniu w celu zapewnienia zgodności z wymaganiami RODO.
- System PAM w wersji wirtualnej musi obsługiwać moduł vTPM (*Virtual Trusted Platform Module*) dla przechowywania kluczy prywatnych użytkowników.
- PAM musi obsługiwać mechanizm awaryjnego dostępu do zaszyfrowanych haseł przechowywanych w systemie na zasadzie procedury „glass breaking”. Wszystkie działania w tym trybie muszą być logowane celem możliwości przeprowadzenia audytu.

- System musi automatycznie nagrywać obraz podczas uruchomienia procedury awaryjnej (glass breaking)
- Automatyczna zmiana hasła konta po poprawnym zalogowaniu
- Wsparcie dla zaplanowanej zmiany haseł według harmonogramu
- Możliwość tworzenia procedury żądania dostępu do haseł i zatwierdzania takich żądań poprzez konfigurowalną ilość administratorów
- Ustawienie dedykowanego dostępu do skonfigurowanego hasła dla jednego administratora. W tym stanie dostęp jest ograniczony tylko dla jednego użytkownika uprzywilejowanego.
- Wymagane jest wsparcie dla algorytmów szyfrowania SSH o wysokiej sile
- Zaawansowany protokół uwierzytelniania RDP, w tym CredSSP i TLS
- Kontrola dostępu oparta na rolach (RBAC)
- Kontrola uprawnień oparta na użytkownikach oraz grupach użytkowników
- Kontrola profili dostępowych w formie polityk
- Wsparcie dla Disaster Recovery
- Użytkownik uprzywilejowany musi mieć możliwość pracy co najmniej w następujących trybach:
    - Agentowy – dostępne wszystkie funkcjonalności. Agent musi być dostępny bezpłatnie
    - Bezagentowo, za pomocą przeglądarki internetowej wraz z dedykowanym rozszerzeniem. Metoda ta musi umożliwiać uzupełnianie haseł przez PAM oraz nagrywanie sesji
    - Bezagentowo, za pomocą przeglądarki internetowej bez dodatkowych rozszerzeń.

Uwierzytelnianie

- Obsługa uwierzytelniania użytkowników za pomocą certyfikatów
- Możliwość korzystania z lokalnej bazy danych użytkowników
- Obsługa uwierzytelniania wieloskładnikowego opartego na SAML
- Obsługa OIDC (openID Connect), SAML
- Obsługa wielu połączeń SAML SP
- Możliwość integracji z istniejącymi usługami uwierzytelniania, w nie mniejszym zakresie niż Active Directory, LDAP, radius.
- Wsparcie dla integracji z istniejącymi systemami zarządzania tożsamościami
- Możliwość obsługi większej liczby kont uprzywilejowanych w miarę rozwoju organizacji
- Dostęp do zasobów użytkowników uprzywilejowanych musi również obejmować możliwości blokady w oparciu o dodatkowe parametry:
    - Kontrola dostępu oparta na adresie źródłowym IP użytkownika

- Ograniczanie dostępu oparte na harmonogramie użytkownika
- Kontrola dostępu do docelowego serwera oparta o przypisane tagi ZTNA (stan stacji, z której następuje połączenie jest badany przez mechanizmy ZTNA)

Licencjonowanie

- Oprogramowanie musi być objęte kompletną licencją producenta na całe rozwiązanie. Nie dopuszcza się dodatkowych wymagań licencyjnych dla systemu operacyjnego, bazy danych, oprogramowania serwera WWW lub podobnych.
- Nie dopuszcza się licencjonowania ilości zasobów, do których realizowany jest nadzorowany dostęp.
- Nie dopuszcza się licencjonowania ilości zajętego miejsca na dysku przez nagrania sesji.
  - Wymagana jest licencja umożliwiająca zestawienie co najmniej 1 równoległej sesji dostępowej, niezależnie od całkowitej liczby zdefiniowanych użytkowników w systemie.
- Licencja musi pozwalać na użytkowanie rozwiązania co najmniej w okresie obowiązywania zakontraktowanej gwarancji wsparcia technicznego.

Monitorowanie i raportowanie

- Możliwość monitorowania aktywności użytkowników z kontami uprzywilejowanymi.
- Generowanie szczegółowych raportów audytowych w celu analizy i śledzenia działań użytkowników

Gwarancja i wsparcie techniczne

Gwarancja wsparcia technicznego i dostępności aktualizacji oprogramowania w celu utrzymania systemu w aktualnym i bezpiecznym stanie musi być zapewniona na **okres min. 12 miesięcy.**

7. **System ochrony stacji roboczych i serwerów (EDR/XDR) – liczba chronionych urządzeń – 5.**

Wspierane systemy operacyjne

System Operacyjny Windows:

<u>Systemy Operacyjne Komputerów</u>

Windows 11

Windows 10

<u>Systemy operacyjne serwera</u>

Windows Server 2025 64x

Windows Server 2022 Core

Windows Server 2022

Windows Server 2019 Core

Windows Server 2019

Windows Server 2016

Windows Server 2016 Core

Systemy Operacyjne Linux i wersja kernel

Oparte o RPM

RHEL 7.x - 3.10.0 (build 957) 64-bit

RHEL 8.x - 4.18.0 64-bit

RHEL 9.x - 5.14.0 64-bit

RHEL 10.x - 6.12.0 64-bit

Oracle Linux 7.x (UEK) - 4.18.0 64-bit

Oracle Linux 7.x (RHCK) - 3.10.0 build 957 64-bit

Oracle Linux 8.x (UEK) - 5.4.17 / 5.15.0 64-bit

Oracle Linux 8.x (RHCK) – 4.18.0 64-bit

Oracle Linux 9.x (UEK) – 5.15.0 64-bit

Oracle Linux 9.x (RHCK) – 5.14.0 64-bit

Oracle Linux 10.x (UEK) - 6.12.0 64-bit

Oracle Linux 10.x (RHCK) - 6.12.0 64-bit

CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit

CentOS 8 Stream - 4.18.0 64-bit

CentOS 9 Stream - 5.14.0 64-bit

CentOS 10 Stream - 6.12.0 64-bit

Fedora 37 – 43 – wsparcie do wygaśnięcia. 64-bit

AlmaLinux 8.x - 4.18.0 64-bit

AlmaLinux 9.x - 5.14.0 64-bit

AlmaLinux 10.x - 6.12.0 64-bit

Rocky Linux 8.x - 4.18.0 64-bit

Rocky Linux 9.x - 5.14.0 64-bit

Rocky Linux 10.x - 6.12.0 64-bit

CloudLinux 7.x - 3.10 (build 957) 64-bit

CloudLinux 8.x - 4.18.0 64-bit

Miracle Linux 8.x - 4.18.0 64-bit

Kylinv10 RHEL - 4.19.90 64-bit

Microsoft Azure Linux 3 – 6.6.64.x.azl3 64-bit

openEuler 24.x - 6.6.0 64-bit

Oparte o Debian

Debian 9 - 4.9.0 32-bit/64-bit

Debian 10 - 4.19 32-bit/64-bit

Debian 11 - 5.10 32-bit/64-bit

Debian 12 – 6.1.0 64-bit

Debian 13 – 6.12 64-bit

Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit

Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 64-bit

Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit

Ubuntu 22.04.x - 5.15 / 5.19 64-bit

Ubuntu 23.04.x – 6.2.0 64-bit

Ubuntu 24.04.x – 6.8.0 64- bit

PopOS 22.04.x – 6.2.6 64-bit

PopOS 24.04.x – 6.17.9 64-bit

Pardus 21 – 5.10.0 64-bit

Mint 20.x – 5.4.0 64-bit

Mint 21.x – 5.15.0 64-bit

Mint 22.x – 6.8.0.x 64-bit

Zorin OS – 6.5.x 64-bit

Linux Mint Debian Edition 6 – 6.1.x 64-bit

Oparte o SUSE

SLES 12 SP4 - 4.12.14-x 64-bit

SLES 12 SP5 - 4.12.14-x 64-bit

SLES 15 SP1 - 4.12.14-x 64-bit

SLES 15 SP2 - 5.3.18-x 64-bit

SLES 15 SP3 - 5.3.18-x 64-bit

SLES 15 SP4 – 5.14.21 64-bit

SLES 15 SP5 – 5.14.21 64-bit

SLES 15 SP6 – 6.4.x 64-bit

SLES 15 SP7 - 6.4.x 64-bit

SLES 16 – 6.12 64-bit

SLED 15 SP4 – 5.14.21 64-bit

openSUSE Leap 15.4 - 15.5 - 5.14.21 64-bit

openSUSE Leap 16 – 6.12 64-bit

Cloud based Linux

AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x 64-bit

Amazon Linux v2 - 4.14.x / 4.19.x / 5.10 64-bit

Amazon Linux 2023 – 6.1.x 64-bit

Google COS Milestones 77, 81, 85 - 4.19.112 / 5.4.49 64-bit

Azure Mariner 2 - 5.15 64-bit

Systemy Operacyjne Mac OS X

macOS Tahoe (26.x)

macOS Sequoia (15.x)

macOS Sonoma (14.x)

macOS Ventura (13.x)

macOS Monterey (12.x)

Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Interfejs oraz pomoc techniczna świadczona w języku polskim.
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi.
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
5. Wbudowana technologia do ochrony przed rootkitami.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. Możliwość ustawienia zadania skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Ochrona krytycznych kluczy rejestru przed ich wykorzystaniem lub nieautoryzowanym dostępem do nich.
13. Możliwość dodawania wykluczeń na podstawie:

a) Plik

b) Folder

c) Rozszerzenie

d) Proces

e) Hash pliku

f) Hash certyfikatu

g) Nazwa zagrożenia

h) Wiersz poleceń

i) IP/maska

14. Skanowanie poczty opartej o protokoły IMAP, MAPI, POP3 i SMTP w czasie rzeczywistym.
15. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie w przeglądarce.
16. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
17. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH, IMAPS, MAPI, POP3S, SMTPS.
18. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.

19. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
20. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia, kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i godziny.
21. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
22. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
23. Administrator musi mieć możliwość ukrycia ikony oprogramowania w obszarze powiadomień systemu Windows.
24. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na punkcie końcowym Windows i macOS.
25. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
26. Oprogramowanie klienckie posiada wbudowaną funkcję do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
27. Możliwość wykorzystania funkcji skanowania lokalnego lub hybrydowego ze sprawdzaniem reputacji plików w chmurze.
28. System musi umożliwiać kontrolę dostępu do urządzeń na podstawie interfejsów, do których zostały one podłączone.
29. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej na podstawie ich wykrycia lub wpisanych ręcznie ID urządzenia lub ID produktu.
30. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.

31. Wbudowany IDS.
32. Możliwość tworzenia list sieci zaufanych.
33. Możliwość dezaktywacji funkcji zapory sieciowej.
34. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
35. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa).
36. Komunikacja między konsolą zarządzającą, a punktami końcowymi jest szyfrowana.
37. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:

a) Możliwość wymuszenia funkcji DEP systemu Windows.

b) Możliwość wymuszenia relokacji modułów (ASLR) dla Windows.

38. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak:

-Pierwszy dostęp.

-Dostęp do poświadczeń.

-Wykrycie.

-Crimeware.

-Ruch boczny.

39. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików w momencie szyfrowania, a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji. Oprogramowanie musi dać możliwość odzyskania plików na żądanie lub automatycznie, o następujących rozszerzeniach:

3fr, ai, arw, bay, cdr, cer, cr2, crt, crw, dcr, der, dll, dng, doc, docm, docx, dwg, dxf, dxg, eps, erf, exe, indd, jpe, jpeg, jpg, mdf, mef, mrw, nef, nrw, odb, odc, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, pdf, pef, pem, pfx, ppt, pptm, pptx, psd, pst, ptx, png, r3d, raf, rtf, rw2, rwl, sr2, srf, srw, wb2, wpd, wps, x3f, xlk, xls, xlsb, xlsm, xlsx, msg, py, ini, xml, msi, cab, tsf, dgn, log, gif, csv, avi, mov, mp4

40. System musi wykrywać podatne sterowniki zainstalowane na punkcie końcowym z Windows.
41. Agent i usługi oprogramowania antywirusowego zainstalowanego na punkcie końcowym muszą być chronione przed próbami manipulacji i naruszenia ich integralności w systemie Windows.
42. System musi umożliwiać skanowanie oprogramowania układowego UEFI.
43. System umożliwia przechwytywanie TLS handshake pozwalając na skanowanie ruchu sieciowego bez konieczności deszyfracji.
44. Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej.
45. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows i macOS do SIEM Splunk (wymaga TLS 1.2 lub wyższy) lub z systemem Windows i Linux do serwera Syslog (JSON).

46. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników naruszeń bezpieczeństwa (IOC).

Stacje robocze i serwery

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.
4. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
5. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.
6. Produkt i zawartość zabezpieczeń powinny być aktualizowane nie rzadziej niż raz na godzinę.
7. Oprogramowanie musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
8. Oprogramowanie musi posiadać możliwość skanowania jedynie nowych i zmienionych plików.
9. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji na systemach Windows po doinstalowaniu odpowiedniego modułu. Zmiana ustawień zabezpieczona jest hasłem.
10. Dla maszyn z systemem Linux możliwość wskazania katalogów, które mogą być chronione w czasie rzeczywistym.

Ochrona Exchange

1. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.
2. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w ciągu określonego czasu.
3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz niemożliwych do przeskanowania.
4. Możliwość skanowania w poszukiwaniu potencjalnie niechcianych aplikacji (PUA).
5. Możliwość skanowania malware wewnątrz archiwów.
6. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen.
7. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.
8. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy.
9. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi.
10. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowanie maila do konkretnej skrzynki pocztowej.

11. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością.
12. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.

Konsola zdalnej administracji

1. System musi umożliwiać centralne zarządzanie i konfigurację ochrony wspieranych stacji roboczych i serwerów.
2. Możliwość integracji wielu domen Active Directory.
3. Możliwość uruchomienia zdalnego skanowania wybranych punktów końcowych.
4. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony punktu końcowego (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania na żądanie, zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
5. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi.
6. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, systemu operacyjnego.
7. Możliwość centralnej aktualizacji punktów końcowych z serwera w sieci lokalnej lub z Internetu.
8. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
9. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
10. Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) oraz wyeksportowanie ich do formatu: pdf i csv. Również zbiorczo w formie archiwum zip.

11. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie.
12. Możliwość generowania raportu co godzinę.
13. Pierwsza aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
14. Możliwość dodania etykiety do stacji roboczej.
15. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
16. Możliwość przechowywania kwarantanny maksymalnie 180 dni.
17. Możliwość definiowania, czy pliki z kwarantanny mają być przesyłane do producenta i co ile godzin ma się ta czynność odbywać.
18. Po aktualizacji zawartości bezpieczeństwa opcja automatycznego przeskanowania kwarantanny.
19. Wsparcie techniczne drogą mailową i telefoniczną w języku polskim od poniedziałku do piątku (w dni robocze) w godzinach 7:30–15:30.
20. Po integracji z lokalnym Active Directory możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
21. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji. Określenie lokalizacji na podstawie:

-Zakres adresów IP/IP.

-Adres bramy.

-Adres serwera WINS.

-Adres serwera DNS.

-Połączenie DHCP sufiksów DNS.

-Punkt końcowy może rozwiązać hosta.

-Typ sieci.

-Nazwa hosta.

22. Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238.
23. Możliwość naprawy instalacji agenta z poziomu konsoli.
24. Możliwość utworzenia reguły, która będzie usuwała punkty końcowe z konsoli zarządzającej, jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn, które automatycznie będą usuwane oraz na określenie godziny, o której te maszyny będą usuwane.
25. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
26. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
27. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux lub MacOS.
28. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
29. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS.

30. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M oraz osobnego pakietu dla systemów Windows z Intel x86 oraz oddzielnego dla architektury ARM.
31. System umożliwia pobieranie plików poddanych kwarantannie z poziomu centralnej konsoli administracyjnej.
32. Możliwość wygenerowania i zapisania logów na stacji roboczej z poziomu konsoli zarządzającej.
33. System pozwala na tworzenie spersonalizowanych komunikatów dla stron zablokowanych przez administratora w oparciu o harmonogram.
34. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
35. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Przypisywanie musi odbywać się ręcznie lub automatycznie. Musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.
36. Ochrona proaktywna oparta o maszynowe uczenie, która działa w fazie poprzedzającej wykonanie. Ochrona ta musi wykrywać zagrożenia takie jak:
    a) Ukierunkowane ataki.
    b) Podejrzane pliki i ruch w sieci.
    c) Exploity.
    d) Ransomware.
    e) Grayware.
37. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego.

38. Moduł ochrony proaktywnej musi działać w trybach, które administrator może dowolnie zmieniać na:
    a) Tolerancyjny.
    b) Normalny.
    c) Agresywny.
39. Zintegrowany sandbox po stronie producenta, który pozwala na analizę pliku:
    a) Plik może zostać wysłany automatycznie ze stacji roboczej, jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora.
    b) Możliwość ręcznego przesłania archiwum zabezpieczonego hasłem.
    c) Możliwość ręcznego przesłania adresu URL.
    d) W przypadku ręcznego przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.
40. Wbudowany sandbox musi działać w trybie monitorowania i blokowania.
41. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja, przeniesienie do kwarantanny lub tylko raportowanie.
42. Wbudowany sandbox musi oferować opcję wstępnego filtrowania plików z kategorii aplikacje, dokumenty, skrypty, archiwa, maile zapisane do pliku, pod kątem podejrzanego zachowania.
43. Wbudowany sandbox musi posiadać opcję, która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.
44. Minimalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 1KB.

45. Maksymalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 50MB.

46. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system, który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100, gdzie liczba mniejsza stanowi mniejsze ryzyko, a liczba większa większe ryzyko. System ponadto musi posiadać:

    a) Funkcję, która pozwala wyszukiwać podatności ustawień punktów końcowych oraz naprawiać je lub ignorować z podziałem na typ wykrytej konfiguracji:

-Przeglądarka

-Sieć

-System operacyjny

-Luki

System ponadto musi określać nasilenie zagrożenia wynikłego z wykrytej podatności w oparciu o punkty procentowe oraz posiadać funkcję cofnięcia wprowadzonych zmian w ustawieniach systemów.

    b) System zarządzania ryzykiem powinien określać luki w wykrytym zainstalowanym oprogramowaniu podając przy tym numer CVE tych luk.

    c) System pozwala na śledzenie i wykrywanie ryzykownych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem o liczbie użytkowników, których takie działanie dotyczy oraz jaka jest jego szkodliwość.

d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.

e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich szkodliwość wyrażona w procentach.

f) System pozwala na wykrywanie podatności w oparciu o standardy bezpieczeństwa zgodne z: CIS v8.0, CMMC 2.0 (US), Cyber Essentials v3.2 (UK), Essential Eight v2023.11 (AU), HIPPA (US), SOC 2, ISO/IEC 27001:2022, PCI DSS v4.0.1, NIST CSF 2.0, GDPR (EU), NIS2 (EU), DORA (EU).

47. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.
48. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.
49. Możliwość zablokowania konta w konsoli, jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.
50. Funkcja pojedynczego logowania – Single Sign-on (SSO) przy integracji z Microsoft Azure.
51. Raport podsumowujący - Możliwość podglądu raportu, który streszcza stan środowiska firmowego w ciągu ostatnich 24h, 7 dni lub 30 dni. Z rozróżnieniem na takie sekcje jak:
    a) Zarządzane punkty końcowe.
    b) Ilość zajętych miejsc w licencji z rozróżnieniem na stacje robocze Windows, serwery Windows, macOS, Linux oraz fizyczne punkty końcowe i maszyny wirtualne.
    c) Pięć rodzajów najczęściej blokowanych zagrożeń.

d) Podział zagrożeń na urządzenia takie jak stacje robocze i serwery.

e) Status incydentów bezpieczeństwa, które wystąpiły.

f) Stan modułów punktów końcowych.

g) Ocena ryzyka firmy.

h) Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.

i) Zablokowane techniki ataku sieciowego z podziałem na takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch boczny, crimeware.

52. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:

a) Raporty

b) Licencjonowanie

c) Konta

d) Pakiety

e) Incydenty

f) Sieć

g) Kwarantanna

h) Integracje

i) Event Push Service

j) Polityki

53. Early access – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Programy wczesnego dostępu powinny umożliwiać testowanie najnowszych funkcji oprogramowania,

których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.

54. Możliwość utworzenia konsoli typu Partner, która pozwala na zarządzanie wieloma firmami z poziomu jednej scentralizowanej konsoli zarządzającej, konsola partnerska musi umożliwiać:
    a) Pobieranie przez partnera plików z kwarantanny podległych firm.
    b) Zarządzanie systemem ochrony firm podrzędnych przez Partnera z jednej konsoli lub tworzenie bezpośrednich dostępów użytkowników dla tych firm.
    c) Odseparowanie przez administratora konsoli podrzędnej od konsoli partnera nadrzędnego.
55. Profil firmy w konsoli typu Partner - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej. Dostępne są kategorie m.in: Lotnictwo, Budownictwo, Edukacja, Służba zdrowia, Handel i inne.
56. System musi umożliwiać wybór trzech poziomów obciążenia procesora dla zadań określonych w harmonogramie skanowania na systemach Windows, Linux i macOS.
57. System musi posiadać funkcję wstrzymywania skanowania podczas pracy na baterii.
58. Konsola administracyjna umożliwia zmianę motywu dla interfejsu spośród jasnego, ciemnego lub wybranego automatycznie w oparciu o ustawienia systemowe.
59. System umożliwia tymczasowe wyłączenie wszystkich lub wybranych modułów ochrony na określony czas, który wynosi 15 minut, 30 minut, 1 godzina, 2 godziny, 4 godziny. Po ponownym uruchomieniu ochrony możliwość przeprowadzenia pełnego skanowania.

60. Centrum integracji – Panel umożliwiający zarządzanie integracjami z rozwiązaniami zewnętrznymi tj. Vmware vCenter, Veeam Backup & Replication, Microsoft Active Directory, Vmware Tanzu, Microsoft Exchange (on-premises), SecurityCoach (KnowBe4).
61. Wbudowany sandbox musi posiadać możliwość przesyłania pliku do analizy z komputera zdalnego za pomocą podanej ścieżki. Wielkość pliku nie może przekraczać 100MB.
62. Filtrowanie wykrytych incydentów bezpieczeństwa m.in. na podstawie:

a) ID.

b) Ostatnia aktualizacja.

c) Status.

d) Osoba przydzielająca.

f) Data utworzenia.

g) Priorytet.

h) Ocena szkodliwości w skali 0-100.

i) Podmioty.

j) Zasoby.

k) Ostatnia faza killchain.

l) Wykonane czynności.

m) Skorelowane incydenty.

n) Typ incydentu.

63. System umożliwia wygenerowanie i pobranie zestawu informacji z chronionych punktów końcowych w formie archiwum. Funkcja powinna być dostępna dla systemów Windows, Linux oraz macOS. Archiwum musi zawierać co najmniej informacje:

    a) Windows

- Logi zainstalowanego agenta.

- Dziennik zdarzeń Windows.

- Informacje o systemie.

- DnsCache.

- Webcache.

- Informacje z głównych katalogów rejestru (SYSTEM, SOFTWARE, DEFAULT, DRIVERS, SAM, SECURITY).

- Harmonogram zadań.

- Historia Powershell (jeśli włączono).

    b) Linux

- Podstawowy log pomocy technicznej zainstalowanego agenta.

- Certyfikaty.

- Autorun i usługi.

- Informacje sieciowe.

- Informacje systemowe.

- Zainstalowane pakiety.

c) macOS

- Podstawowy log pomocy technicznej zainstalowanego agenta.

- Autorun.

- Lista procesów.

- Informacje sieciowe.

- Informacje o systemie.

64. Oprogramowanie musi umożliwiać przegląd konfiguracji punktów końcowych w czasie rzeczywistym poprzez tworzenie zapytań pod kątem wykrywania:

a) historia powłoki.

b) wczytywanie bibliotek .dll z podejrzanej lokalizacji.

c) Sesje logowania z użyciem jawnych danych uwierzytelniających.

d) Arp cache.

e) Ip forwarding.

f) Lista zamontowanych nośników.

g) Konfiguracja ip tables.

h) Połączenia TLS które używają certyfikatów self-signed.

i) Używane rozszerzenia w przeglądarce Chrome.

j) Używane rozszerzenia w przeglądarce Firefox.

k) Używane rozszerzenia w przeglądarce Safari.

l) Źródła apt w systemach Linux.

m) Wyświetlanie zainstalowanych pakietów DEB.

n) Wyświetlanie zainstalowanych pakietów RPM.

o) Pakiety Python zainstalowane w systemie.

p) Lista użytkowników, którzy zostali utworzeni w ciągu ostatnich 30 dni (Linux).

q) Wykrywanie czy aplikacje zdalnego dostępu są zainstalowane w systemie MacOS.

r) Wykrywanie czy Kontrola Kont Użytkowników (UAC) jest wyłączona.

s) Wykrywanie czy SecureBoot jest włączony.

t) Lista zapamiętanych sieci bezprzewodowych.

u) Wykrywa, czy zmienił się domyślny folder startowy użytkownika.

w) Wykrywa, czy zmienił się domyślny folder startowy maszyny.

65. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych reguł, po spełnieniu których może zostać wygenerowany incydent bezpieczeństwa. Funkcja ta powinna:

a) Oferować opcję podjęcia automatycznych działań po spełnieniu warunków tj.: izolacja punktu końcowego, wygenerowanie archiwum diagnostycznego, przesłanie pliku do analizy sandbox, zakończenie procesu i innych.

b) Automatyczne działania zapobiegawcze są zależne od wyboru kategorii.

c) Tworzenie reguł musi być określone poprzez wybór operatora np. „to", „zawiera", „jest jednym z" itp.

d) Dotyczyć określonych kryteriów tj. proces, plik, rejestr, połączenia.

e) Zapewniać możliwość tworzenia zapytań YARA.

f) Umożliwiać określenie priorytetu kolejności automatyzacji.

g) Administrator powinien mieć możliwość wyboru poziomu szkodliwości potencjalnie wygenerowanych incydentów (wysokie, średnie i niskie).

EDR-Endpoint Detection and Response

Produkt zapewnia szczegółowe informacje o wykrytych incydentach, interaktywną mapę incydentów i działania naprawcze.

Komponenty EDR

Główne elementy:

1. Sensor EDR, który gromadzi i przetwarza dane dotyczące punktu końcowego i zachowania aplikacji w celu ich raportowania.
2. Analityka Bezpieczeństwa, komponent służący do interpretacji metadanych gromadzonych przez sensor EDR.
3. Możliwość instalacji dodatkowego, dedykowanego agenta z sensorem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną równolegle ochronę świadczoną przez innego producenta oprogramowania antywirusowego.

Wykrywanie podejrzanej aktywności

Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności.

1. Bazowanie na systemach opartych o techniki MITRE ATT&CK i własnej inteligencji.
2. Zgłaszanie naruszeń jako incydent w module EDR.

Badanie incydentów i wizualizacja

1. Produkt zapewnia wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym czasie.
2. Produkt integruje się z bazą wiedzy MITRE ATT&CK i odpowiednio oznacza zdarzenia bezpieczeństwa.
3. Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi danymi lub działaniami z następującymi informacjami:
   a) Karta podsumowująca zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia.
   b) Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej.
   c) System gromadzi informacje o działaniach podejmowanych przez produkt w związku ze zdarzeniem bezpieczeństwa.

Incydenty

1. Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i chronologicznej linii zdarzeń oraz daje możliwość:
    a) Filtrowania zdarzeń.
    b) Zakończenia procesów.
    c) Dodania procesów do czarnej listy.
    d) Dodania procesów do białej listy.
    e) Izolacji hosta.
    f) Przesłania pliku do Sandbox.
    g) Sprawdzenia informacji o pliku w Google.
    h) Sprawdzenia informacji o pliku w VirusTotal.
2. Możliwość szybkiego podglądu incydentów za pomocą spersonalizowanych widoków list lub widoku domyślnego.
3. System umożliwia blokowanie na podstawie utworzonych reguł czarnej listy przy pomocy kategorii:

a) Hash MD5 lub SHA256.

b) Pełna ścieżka do aplikacji.

c) Reguła połączenia.

4. Możliwość importu reguł czarnej listy dla hash, ścieżek do aplikacji oraz reguł połączeń z pliku CSV.

5. System musi oferować szeroki zakres filtrowania dodanych reguł blokowania minimum po nazwie pliku, hash pliku, typu hash, ścieżce, protokole, porcie/zakresie portów, daty dodania.
6. Możliwość wygenerowania i wyeksportowania listy incydentów do pliku .csv.

Patch Management/Zarządzanie Aktualizacjami

Wspierane systemy operacyjne Windows:

- Windows 11
- Windows 10
- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Wspierane systemy operacyjne Linux (64-bit):

- CentOS 7 – GA+ (7.2003)
- Red Hat Enterprise Linux RHEL 7 – GA+ (7.1-7.9)
- Red Hat Enterprise Linux REL 8 – GA+ (8.4)
- SUSE Linux Enterprise SLES 12 – GA+ (SP5)
- SUSE Linux Enterprise SLES 15 – GA+ (SP5)
- SUSE Linux Enterprise SLED 15 – GA+ (SP5)

Wspierane systemy operacyjne macOS:

- macOS Tahoe (26.x)
- macOS Sequoia (15.x)
- macOS Sonoma (14.x)
- macOS Ventura (13.x)
- macOS Monterey (12.x)

Wymagany Pełny Dostęp do Dysku.

1) Możliwość działania w trybie automatycznym:
   a) Możliwość wykrycia i wylistowania brakujących kompatybilnych łatek.
   b) Możliwość zaplanowania oddzielnej automatycznej instalacji w oparciu o kategorię poprawek (bezpieczeństwo / niezwiązane z zabezpieczeniami).
   c) Możliwość opóźnienia ponownego uruchomienia, jeśli instalacja łatki tego wymaga.
2) Rozwiązanie musi zezwalać na tryb manualny – wykrywanie i instalacja łatek na żądanie.
3) Rozwiązanie musi oferować możliwość podejrzenia wszystkich kompatybilnych brakujących łatek ze wspieranych punktów końcowych. Informacje te zostaną zebrane w zakładce inwentarza aktualizacji.
   a) Rozwiązanie umożliwia sprawdzenie, które punkty końcowe posiadają zainstalowane lub brakujące aktualizacje.
   b) Rozwiązanie przesyła informacje zwrotne w przypadku niepowodzenia instalacji łatki.
   c) Rozwiązanie daje użytkownikowi możliwość szybkiej instalacji brakujących łatek na urządzeniu.

d) Administrator powinien mieć możliwość dodania do czarnej listy jednej lub wielu łatek.

4) Rozwiązanie raportuje brakujące łatki z perspektywy punktu końcowego (zainstalowane/ brakujące na każdym punkcie końcowym).

5) Rozwiązanie zapewnia możliwość pobierania aktualizacji poprzez serwer pośredniczący dla systemu Windows lub bezpośrednio przez Internet.

6) Funkcja skanowania dostępnych aktualizacji dla nowo zainstalowanych kompatybilnych aplikacji na punkcie końcowym.

7) System musi umożliwiać wyświetlenie listy numerów CVE dla podatności naprawianych przez daną aktualizację.

8. Usługa centralnego gromadzenia, przechowywania, analizy i raportowania logów

Opis przedmiotu zamówienia

Przedmiot zamówienia: świadczenie przez okres minimum 12 miesięcy usługi centralnego gromadzenia, przechowywania, analizy i raportowania logów pochodzących z posiadanych przez Zamawiającego urządzeń bezpieczeństwa sieciowego.

Główny kod CPV: 72317000-0 – Usługi przechowywania danych.
Dodatkowe kody CPV: 72316000-3 – Usługi analizy danych; 72611000-6 – Usługi w zakresie wsparcia technicznego; 72263000-6 – Usługi wdrażania oprogramowania.

Lp.	Obszar	Minimalne wymaganie Zamawiającego	Sposób potwierdzenia / odbioru
1	Rodzaj świadczenia	Usługa centralnego gromadzenia, przechowywania, analizy i raportowania logów z urządzeń bezpieczeństwa sieciowego eksploatowanych przez Zamawiającego	Oświadczenie Wykonawcy / opis oferowanej usługi
2	Okres świadczenia	Usługa świadczona przez min. **12 miesięcy** od dnia jej uruchomienia i odbioru przez Zamawiającego	Umowa lub OPZ / protokół uruchomienia

3	Model usługi	Usługa świadczona z infrastruktury utrzymywanej przez Wykonawcę, bez konieczności zakupu i instalacji przez Zamawiającego dedykowanego urządzenia do centralnego składowania i analizy logów	Oświadczenie Wykonawcy
4	Lokalizacja infrastruktury	Infrastruktura, na której przechowywane są logi Zamawiającego, musi znajdować się w **centrum danych zlokalizowanym na terytorium Polski**	Oświadczenie Wykonawcy
5	Obsługiwane środowisko	Usługa musi umożliwiać odbieranie i przetwarzanie logów z posiadanych przez Zamawiającego urządzeń **bezpieczeństwa sieciowego** bez konieczności ich wymiany	Test podczas uruchomienia
6	Liczba urządzeń	Usługa musi obejmować **urządzenie /urządzenia sieciowe** wskazane przez Zamawiającego (w ilości nie większej niż 7 urządzeń)	Wykaz urządzeń / protokół
7	Separacja środowiska	Wykonawca musi zapewnić Zamawiającemu **dedykowaną logiczną domenę administracyjną** przeznaczoną wyłącznie dla urządzeń i danych	Prezentacja środowiska po uruchomieniu

		Zamawiającego, zapewniającą logiczną separację od środowisk innych klientów Wykonawcy	
8	Separacja uprawnień	Dostęp użytkowników Zamawiającego musi być ograniczony do urządzeń i danych przypisanych do jego wydzielonej domeny administracyjnej	Test konta Zamawiającego
9	Pojemność	Dla wydzielonego środowiska Zamawiającego należy zapewnić **150 GB przestrzeni przeznaczonej na logi**	Widok parametrów przydzielonego środowiska lub oświadczenie Wykonawcy
10	Logi Analytics	System musi umożliwiać skonfigurowanie przechowywania logów w warstwie analitycznej przez okres **do 60 dni**, w ramach przydzielonej pojemności	Prezentacja ustawień polityki retencji
11	Logi Archive	System musi umożliwiać skonfigurowanie przechowywania logów w warstwie archiwalnej przez okres **do 365 dni**, w ramach przydzielonej pojemności	Prezentacja ustawień polityki retencji

12	Zasada retencji	Okresy 60 dni dla Analytics i 365 dni dla Archive określają maksymalne wartości konfigurowanej polityki retencji. Faktyczny okres zachowania danych jest ograniczony przydzieloną przestrzenią min. **150 GB** i może zależeć od rzeczywistego wolumenu logów generowanych przez urządzenia Zamawiającego	Prezentacja ustawień polityki retencji Akceptacja warunków usługi
13	Gromadzenie logów	Usługa musi umożliwiać centralne odbieranie i przechowywanie logów przesyłanych przez objęte zamówieniem urządzenia Zamawiającego	Wygenerowanie zdarzenia testowego na każdym podłączonym urządzeniu i potwierdzenie jego odebrania
14	Analityka	Dla danych znajdujących się w warstwie Analytics usługa musi umożliwiać przeglądanie, wyszukiwanie, filtrowanie i analizowanie zgromadzonych logów	Test funkcjonalny po uruchomieniu
15	Zakres logowania	Usługa musi umożliwiać konfigurację zakresu zdarzeń/logów podlegających przesyłaniu i analizie	Prezentacja konfiguracji

16	Raportowanie	Usługa musi umożliwiać generowanie raportów na podstawie logów znajdujących się w warstwie Analytics	Wygenerowanie raportu testowego
17	Zawartość raportów	Usługa musi umożliwiać konfigurację zakresu oraz zawartości generowanych raportów	Prezentacja konfiguracji
18	Format raportów	Usługa musi umożliwiać generowanie lub eksport raportów co najmniej w formacie **PDF** oraz **XML** lub w formatach funkcjonalnie równoważnych umożliwiających zapis i dalsze wykorzystanie raportu	Wygenerowanie pliku testowego
19	Obsługa zdarzeń	Usługa musi zapewniać mechanizm definiowania i obsługi zdarzeń na podstawie logów analitycznych, pozwalający na automatyczne wykrycie spełnienia określonych warunków – mechanizm klasy **Event Handler lub funkcjonalnie równoważny**	Prezentacja funkcji / utworzenie przykładowej reguły
20	Uruchomienie środowiska	W ramach zamówienia Wykonawca utworzy i skonfiguruje wydzielone środowisko Zamawiającego, w tym przydzieli wymaganą przestrzeń i skonfiguruje parametry retencji	Protokół uruchomienia

21	Podłączenie urządzeń	W ramach uruchomienia usługi Wykonawca wykona czynności niezbędne do podłączenia do usługi urządzeń wskazanych przez Zamawiającego, w zakresie uzgodnionym z Zamawiającym	Potwierdzenie odbioru logów z każdego urządzenia
22	Test uruchomieniowy	Za skuteczne podłączenie urządzenia uznaje się odebranie przez usługę co najmniej jednego prawidłowego zdarzenia testowego wygenerowanego przez dane urządzenie	Test odbiorowy
23	Utrzymanie platformy	Utrzymanie infrastruktury sprzętowej i programowej wykorzystywanej do realizacji usługi leży po stronie Wykonawcy i nie wymaga wykonywania czynności administracyjnych na platformie bazowej przez Zamawiającego	Oświadczenie Wykonawcy
24	Kanały wsparcia	Wykonawca zapewni obsługę zgłoszeń co najmniej za pośrednictwem **poczty elektronicznej i telefonu**	Dane kontaktowe przekazane przy uruchomieniu

25	Limit wsparcia	W ramach zamówienia Wykonawca zapewni **15 godzin wsparcia technicznego w okresie 12 miesięcy**	Ewidencja wykorzystania godzin
26	Okres dostępności supportu	Wsparcie świadczone będzie w trybie **8 godzin dziennie w godzinach od 7.30 do 15.30 w dni robocze / 5 dni w tygodniu przez okres obowiązywania usługi**;	Zapisy umowy lub OPZ
27	Dostęp Zamawiającego	Zamawiający otrzyma dostęp administracyjny/użytkowy do swojego wydzielonego środowiska w zakresie niezbędnym do przeglądania i analizy danych oraz korzystania z funkcji raportowych	Test logowania
28	Zakończenie wdrożenia	Etap uruchomienia uznaje się za wykonany po utworzeniu wydzielonego środowiska, skonfigurowaniu wymaganych parametrów, podłączeniu wszystkich urządzeń objętych zamówieniem i pozytywnym zakończeniu testu odbierania logów	Protokół odbioru

9. Zakres wdrożenia

Szafa rack 19" 27U 800x1000 wraz z okablowaniem

Poz. 1. Szafa teleinformatyczna rack 19", stojąca, 27U

Parametr	Wymagany minimalny parametr
Typ	Szafa stojąca, jednosekcyjna, do samodzielnego montażu (flat pack)
Standard	19", zgodność z ANSI/EIA RS-310D, IEC 297-2, DIN 41494 część 1 i 7, ETSI
Wysokość użytkowa	27U
Szacunkowe wymiary zewnętrzne (szer. x gł. x wys.)	800 x 1000 x ok. 1431–1461 mm
Rozstaw szyn 19"	Wewnętrzny rozstaw montażowy 450 mm; szyny z pełną regulacją głębokości
Konstrukcja	Stal, grubość profili min. 2 mm

Parametr	Wymagany minimalny parametr
Nośność statyczna	Min. 800 kg
Drzwi przednie	Perforowane, metalowe, jednoskrzydłowe, zamykane na klucz
Drzwi tylne	Perforowane, metalowe, zapewniające efektywną wentylację wnętrza, zamykane na klucz
Panel górny/dolny	Wyłamania (przepusty kablowe) umożliwiające górne i dolne wprowadzenie okablowania
Panel LCD	Zintegrowany panel LCD/termostat cyfrowy z funkcją odczytu temperatury i sterowania wentylacją
Wentylacja	Panel wentylacyjny w obudowie górnej wyposażony w wentylatory 230V (min. 4 szt.)
Podstawa/mobilność	Panel podłogowy z min. 4 kółkami jezdnymi z hamulcem oraz regulowanymi nóżkami poziomującymi

Parametr	Wymagany minimalny parametr
Klasa szczelności	IP20
Uziemienie	Fabrycznie przygotowane punkty uziemienia szafy i drzwi (bonding)
Gwarancja	**Min. 36 miesięcy**
Model referencyjny	Lanberg FF01-8027-23BL lub produkt równoważny spełniający wszystkie ww. parametry

Ilość: 1 szt.

Poz. 2. Okablowanie i wyposażenie towarzyszące

Wykonawca zobowiązany jest dostarczyć wraz z szafą rack kompletny zestaw okablowania i akcesoriów niezbędnych do prawidłowego podłączenia i uruchomienia wszystkich dostarczanych w ramach zamówienia urządzeń, w szczególności:

Lp.	Element	Wymagania minimalne
1	Listwa zasilająca PDU rack 19"	Min. 1U, min. 8 gniazd C13 (lub zgodnie z zapotrzebowaniem mocowym dostarczanych urządzeń), z wyłącznikiem/zabezpieczeniem, przewód zasilający min. 2 m
2	Patchpanel 19"	Kat. 6/6A (zgodnie z klasą okablowania sieciowego zastosowaną w rozwiązaniu), liczba portów dostosowana do liczby podłączanych urządzeń, wraz z organizatorem kabli 1U
3	Patchcordy sieciowe	Kat. 6/6A, długości dobrane do rzeczywistych tras w szafie (od urządzeń do patchpanela oraz od patchpanela do switcha), w ilości odpowiadającej liczbie portów aktywnych urządzeń
4	Kable/patchcordy zasilające C13/C14	W ilości odpowiadającej liczbie zasilaczy dostarczanych urządzeń (dla urządzeń z redundantnymi zasilaczami – podwójny komplet), długość dostosowana do rozmieszczenia w szafie
5	Kable światłowodowe (patchcordy SM/MM)	Jeśli wymagane przez konfigurację kart sieciowych/przełączników – zgodne z zastosowanymi transceiverami (SR/LR), z odpowiednim typem złącza (LC/LC, LC/SC)

Lp.	Element	Wymagania minimalne
6	Organizery kabli poziome i pionowe	W ilości zapewniającej uporządkowane prowadzenie okablowania wewnątrz szafy
7	Uziemienie/bonding	Przewód uziemiający szafy oraz elementy bondingowe do połączenia drzwi/szyn z konstrukcją
8	Opaski/rzepy montażowe	Do organizacji i mocowania wiązek kablowych

Wymagania dodatkowe:

1. Dobór typów, długości i ilości okablowania musi zostać dostosowany przez Wykonawcę do rzeczywistej konfiguracji i rozmieszczenia dostarczanych urządzeń w szafie, w sposób zapewniający pełną funkcjonalność i możliwość uruchomienia całego dostarczonego systemu bez konieczności zakupu dodatkowych elementów przez Zamawiającego.
2. Całość okablowania musi zostać poprowadzona i zapięta w sposób uporządkowany (z wykorzystaniem organizerów), z opisem/oznaczeniem obu końców kabla.
3. Wykonawca odpowiada za dostawę, montaż szafy oraz wykonanie okablowania strukturalnego i zasilającego w miejscu wskazanym przez Zamawiającego.
4. **Wykonawca przedstawi protokół z testu okablowania (dla okablowania miedzianego – wynik testera certyfikującego, dla światłowodowego – pomiar tłumienności).**

10. Zakres wdrożenia

Zakres wdrożenia:

1. Montaż i uporządkowanie infrastruktury w szafie rack.
2. Instalacja serwera, dwóch NAS-ów, przełączników, UPS-a oraz elementów zasilających.
3. Wykonanie i uporządkowanie połączeń sieciowych:
    - 10 GbE SFP+ pomiędzy serwerem a przełącznikami,
    - 10 GbE SFP+ pomiędzy przełącznikami,
    - 1 GbE RJ45 pomiędzy NAS-ami a przełącznikami,
    - połączenia zarządzające urządzeń.
4. Konfiguracja dwóch przełączników, połączenia redundantnego oraz wymaganych sieci VLAN.
5. Konfiguracja redundantnych połączeń NAS-ów z wykorzystaniem dwóch portów 1 GbE – agregacja łączy lub failover.
6. Konfiguracja interfejsów zarządzających serwera, NAS-ów, przełączników i UPS-a.
7. Aktualizacja oprogramowania układowego oraz podstawowa konfiguracja serwera.
8. Konfiguracja kontrolera i przestrzeni dyskowej serwera.
9. Instalacja i podstawowa konfiguracja platformy wirtualizacyjnej.
10. Utworzenie i konfiguracja maszyn wirtualnych:

- kontrolera domeny,
- PAM VM,
- dodatkowej maszyny wirtualnej do zastosowań środowiskowych.

11. Uruchomienie kontrolera domeny Active Directory wraz z podstawową konfiguracją DNS, synchronizacji czasu i polityk domenowych.

12. Podstawowa konfiguracja obu NAS-ów:

- konfiguracja interfejsów sieciowych,
- utworzenie puli dyskowych i macierzy RAID,
- utworzenie wolumenów,
- konfiguracja kont administracyjnych,
- konfiguracja powiadomień i monitorowania stanu urządzeń.

13. Instalacja i podstawowa konfiguracja z XDR
14. Wdrożenie i podstawowa konfiguracja PAM VM
15. Podłączenie urządzenia sieciowego klienta do usługi usługi centralnego gromadzenia, przechowywania, analizy i raportowania logów pochodzących z posiadanych przez Zamawiającego urządzeń bezpieczeństwa sieciowego oraz weryfikacja odbioru logów.
16. Konfiguracja monitorowania UPS-a i reakcji środowiska na długotrwały zanik zasilania.
17. Wykonanie testów komunikacji, redundancji i działania podstawowych usług.
18. **Przygotowanie podstawowej dokumentacji powykonawczej oraz przekazanie środowiska klientowi.**

Informacja.
1) Jeżeli w treści zapytania ofertowego lub w załącznikach (w tym w OPZ) wskazano znaki towarowe, patenty, pochodzenie, źródło, szczególny proces, normy, oceny techniczne, specyfikacje techniczne lub systemy referencji technicznych, należy przyjąć, że wskazaniu takiemu towarzyszy dopuszczenie rozwiązań równoważnych. Wskazania te służą wyłącznie określeniu minimalnego standardu jakościowego, technicznego, funkcjonalnego, wydajnościowego lub bezpieczeństwa.
2) Za rozwiązanie równoważne Zamawiający uzna rozwiązanie o takim samym przeznaczeniu, zapewniające parametry, funkcjonalności, jakość, wydajność, poziom bezpieczeństwa, kompatybilność i interoperacyjność nie gorsze niż wymagania minimalne, kompatybilne z pozostałymi elementami przedmiotu zamówienia oraz ze środowiskiem Zamawiającego w zakresie opisanym w opisie przedmiotu zamówienia, niewymagające od Zamawiającego poniesienia dodatkowych nakładów ani zmiany posiadanej infrastruktury.

3) Ocena równoważności dokonywana jest w odniesieniu do wymagań wskazanych w opisie przedmiotu zamówienia, z uwzględnieniem celu, jakiemu dane rozwiązanie ma służyć. Nie podlegają porównaniu cechy właściwe wyłącznie dla konkretnego rozwiązania lub producenta, takie jak nazwy handlowe, zastrzeżone patenty, własnościowe rozwiązania technologiczne lub własnościowe protokoły, o ile zaoferowane rozwiązanie zapewnia realizację wymaganych funkcjonalności w sposób równoważny.
4) W przypadku wymagań dotyczących norm i certyfikatów Zamawiający dopuszcza certyfikaty równoważne, tj. dokumenty wydane przez niezależną jednostkę certyfikującą lub inny uprawniony podmiot, potwierdzające spełnienie wymagań o zakresie merytorycznym odpowiadającym co najmniej wskazanej normie lub certyfikatowi i na co najmniej takim samym poziomie zaawansowania.
5) Ciężar wykazania równoważności spoczywa na Wykonawcy. Wykonawca oferujący rozwiązanie równoważne przedstawia wraz z ofertą opis tego rozwiązania oraz dokumenty potwierdzające jego równoważność, w szczególności karty katalogowe, dokumentację techniczną producenta, oświadczenie producenta, wyniki testów lub certyfikaty.