Załącznik nr 1 do SWZ

**Opis przedmiotu zamówienia**

**Oprogramowanie do tworzenia i zabezpieczania kopii zapasowych – 1 sztuka**

1. **Oprogramowanie musi wspierać co najmniej systemy operacyjne:**

* Windows XP i nowsze
* Windows Server 2003 i nowsze
* Windows SBS 2011/2008, 2003/2003R2
* Windows MultiPoint Server 2012/2011/2010
* Linux

1. **Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:**

* Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www
* Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego).
* Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych.
* Moduł raportujący z możliwością zdefiniowania zawartości, formy częstotliwości generowania raportów oraz metody ich dostarczania

(wysyłanie na podany adres email lub zapisywanie do wskazanego folderu)

* Możliwość definiowania uprawnień dla administratorów system kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.).
* Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami.
* Wsparcie dla Single Sign On dla logowania do systemu.
* Możliwość zarządzania procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT.
* Możliwość definiowania planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem).
* Możliwość tworzenia zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych.
* Możliwość zdalnej instalacji agentów kopi zapasowych z poziomu konsoli cyberochrony na maszynach z systemem operacyjnym Windows.
* Możliwość zdalnego uaktualniania agentów kopi zapasowych.
* Możliwość zdalnego zarządzania procesem wykonywania kopii zapasowej i odzyskiwania danych.
* Możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej).
* Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych.
* Centralny katalog wszystkich danych zapisanych w kopiach zapasowych
* Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.

1. **Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:**

* Kopie zapasowe całych dysków i partycji
* Kopie zapasowe wybranych plików i folderów
* Kopia zapasowa udziałów sieciowych
* Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory)
* Kopie zapasowe baz danych Oracle.
* Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych.
* Zapis kopi zapasowych na udziały sieciowe.
* Zapis kopi zapasowych na serwer SFTP
* Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana.
* Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery), wraz z wsparciem LTO-9.
* Możliwość wyszukiwania plików w kopiach zapasowych
* Możliwość szyfrowania plików kopi zapasowych.
* Wsparcia dla technologii VSS.
* Deduplikacja kopii zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć.
* Kompresja plików kopi zapasowych.
* Możliwość replikacji kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy).
* Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.

1. **Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:**

* Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore.
* Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową.
* Odtworzenie poszczególnych plików i folderów.
* Automatyzacja procesu odtwarzania całych maszyn – np.: po zbootowaniu maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania).
* Granularne odtwarzanie baz danych Microsoft Exchange.
* Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange.
* Wyszukiwanie i podgląd odtwarzanych wiadomości email.
* Granularne odtwarzanie baz danych Microsoft SQL.
* Możliwość granularnego odtwarzania witryn i plików Microsoft SharePoint.
* Odtwarzanie kontrolerów domeny Microsoft Active Directory.
* Granularne odtwarzanie baz danych Oracle.
* Przywracanie przyrostu względem danych, które już się znajdują na dysku na który przywracana jest kopia zapasowa.

1. **Dodatkowe (obowiązkowe) wymagania związane ochroną danych dla systemów Windows 7 i nowszych:**

* Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń.
* Skanowanie oprogramowania celem poszukiwania podatności. Podatności wypisane muszą być z minimum informacjami takimi jak nazwa produktu który zawiera podatność, maszyny na których znaleziono takie oprogramowanie, stopień ważności w skali CVSS.

1. **Przestrzeń chmurowa dostarczana wraz z oprogramowaniem musi spełniać poniższe wymagania:**

* W przypadku uzyskania uzasadnionej pewności, że doszło do naruszenia

bezpieczeństwa, producent oprogramowania bez zbędnej zwłoki dostarczy informacje o takowym naruszeniu na adres e-mail podany podczas rejestracji konta.

* W przypadku wyżej wymienionego naruszenia, producent podejmie kroki, aby

udokumentować, naprawić i zminimalizować skutki naruszenia bezpieczeństwa w odniesieniu do danych osobowych oraz aby zapobiec jego powtórzeniu.

* Kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich repliki muszą być przechowywane na terenie Polski.
* Producent przechowuje dane osobowe klienta (dane osobowe oraz kopie zapasowe) przy użyciu technik szyfrowania, minimum AES-256.
* Producent nie wykorzystuje danych osobowych klienta bez anonimizacji w

środowiskach programistycznych lub testowych.

* Producent oprogramowania przeprowadza okresowe oceny ryzyka i przeglądy co najmniej raz w roku.
* Infrastruktura (chmurowy magazyn kopii zapasowych) jest zaprojektowana zgodnie z podejściem N+1 (to, co niezbędne +1).
* Producent oprogramowania jest zgodny z standardem bezpieczeństwa ISO 27001 lub SOC 2, a magazyn kopii zapasowych musi być zgodny z certyfikatami ISO 9001, ISO 27001 oraz certyfikację DCOS na minimum 4 poziomie.
* Przestrzeń chmurowa dostarczana wraz z oprogramowaniem to minimum 250GB w ramach jednej licencji, na cały okres jej trwania.

1. **Wymagania co do modelu licencjonowania rozwiązania:**

* Możliwość zakupu licencji subskrypcyjnych w okresie 1/3/5 lat
* Model licencjonowania oparty na maszynach fizycznych – brak limitów na chronioną ilość danych i aplikacji.

1. **Oprogramowanie musi wspierać fizyczne i wirtualne komputery z systemem**

**operacyjnym Windows XP i nowsze oraz systemy macOS.**

1. **Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:**

* Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www.
* Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego).
* Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych.
* Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu).
* Możliwość definiowania uprawnień dla administratorów systemu kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.).
* Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami.
* Wsparcie dla Single Sign On dla logowania do systemu.
* Możliwość zarządzania procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT.
* Możliwość definiowania planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem)
* Możliwość tworzenia zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych
* Możliwość zdalnej instalacji agentów kopi zapasowych z poziomu konsoli cyberochrony na maszynach z systemem operacyjnym Windows.
* Możliwość zdalnego uaktualniania agentów kopi zapasowych
* Możliwość zdalnego zarządzania procesem wykonywania kopii zapasowej i odzyskiwania danych.
* Możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej).
* Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych.
* Centralny katalog wszystkich danych zapisanych w kopiach zapasowych.
* Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.

1. **Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:**

* Kopie zapasowe całych dysków i partycji.
* Kopie zapasowe wybranych plików i folderów.
* Kopia zapasowa udziałów sieciowych.
* Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych.
* Zapis kopi zapasowych na udziały sieciowe.
* Zapis kopi zapasowych na serwer SFTP.
* Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana.
* Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery).
* Możliwość wyszukiwania plików w kopiach zapasowych.
* Możliwość szyfrowania plików kopi zapasowych.
* Wsparcia dla technologii VSS.
* Deduplikacja kopi zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć.
* Kompresja plików kopi zapasowych.
* Możliwość replikacji kopi zapasowych na kolejne nośniki (dyski, magazyn chmurowy).
* Możliwość replikacji kopi zapasowych na nośniki taśmowe.
* Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.

1. **Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:**

* Odtworzenie całej maszyny (Windows, Mac) – tzw. Bare Metal Restore.
* Odtworzenie całej maszyny (Windows, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową.
* Odtworzenie poszczególnych plików i folderów.
* Przywracanie przyrostu względem danych, które już się znajdują na dysku na który przywracana jest kopia zapasowa.
* Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowaniu maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania).

1. **Dodatkowe (obowiązkowe) wymagania związane ochroną danych dla systemów Windows 7 i nowszych:**

* Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń
* Skanowanie oprogramowania celem poszukiwania podatności. Podatności wypisane muszą być z minimum informacjami takimi jak nazwa produktu który zawiera podatność, maszyny na których znaleziono takie oprogramowanie, stopień ważności w skali CVSS

1. **Przestrzeń chmurowa dostarczana wraz z oprogramowaniem musi spełniać poniższe wymagania:**

* W przypadku uzyskania uzasadnionej pewności, że doszło do naruszenia bezpieczeństwa, producent oprogramowania bez zbędnej zwłoki dostarczy informacje o takowym naruszeniu na adres e-mail podany podczas rejestracji konta.
* W przypadku wyżej wymienionego naruszenia, producent podejmie kroki, aby udokumentować, naprawić i zminimalizować skutki naruszenia bezpieczeństwa w odniesieniu do danych osobowych oraz aby zapobiec jego powtórzeniu
* Kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich repliki muszą być przechowywane na terenie Polski.
* Producent przechowuje dane osobowe klienta (dane osobowe oraz kopie

zapasowe) przy użyciu technik szyfrowania, minimum AES-256

* Producent nie wykorzystuje danych osobowych klienta bez anonimizacji w

środowiskach programistycznych lub testowych.

* Producent oprogramowania przeprowadza okresowe oceny ryzyka i przeglądy co najmniej raz w roku.
* Infrastruktura (chmurowy magazyn kopii zapasowych) jest zaprojektowana

zgodnie z podejściem N+1 (to, co niezbędne +1).

* Producent oprogramowania jest zgodny z standardem bezpieczeństwa ISO 27001 lub SOC 2, a magazyn kopii zapasowych musi być zgodny z certyfikatami ISO 9001, ISO 27001 oraz certyfikację DCOS na minimum 4 poziomie.
* Przestrzeń chmurowa dostarczana wraz z oprogramowaniem to minimum 50GB w ramach jednej licencji, na cały okres jej trwania.

1. **Wymagania co do modelu licencjonowania rozwiązania**

* Możliwość zakupu licencji subskrypcyjnych w okresie 1/3/5 lat
* Model licencjonowania oparty na maszynach fizycznych – brak limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji)

1. **Serwer z niezbędnym osprzętem – 1 sztuka**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | * Obudowa Rack o wysokości max 1U * 4 wnęk na dyski 3.5” * Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serweraw tym adres IP karty zarządzającej * Obudowa wyposażona 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 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. |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| **Procesor** | * Zainstalowany jeden procesor min. 16-rdzeniowy, min. 2.0GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 265 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| **RAM** | * 4x 32GB DDR5 RDIMM 5600MT/s, |
| **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 |
| **Dyski twarde** | * Zainstalowane:   + 4x dysk SAS o pojemności min. 8TB, Hot-Plug * Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB z możliwością konfiguracji RAID 1. |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT |
| **Wbudowane porty** | * 4 porty USB w tym:   + 1 port USB 3.0 z tyłu obudowy,   + 1 port micro USB z przodu obudowy * 2 port VGA z czego jeden z przodu obudowy * Możliwość rozbudowy o port RS232 |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| **Zasilacze** | * Redundantne, Hot-Plug min. 700W klasy Titanium |
| **Elementy montażowe** | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |
| **System operacyjny/dodatkowe oprogramowanie** | * Windows Server 2025 Standard * 25x licencja dostępowa Windows Server 2025/2022 User CALs * Microsoft SQL Server 2022 Standard, OEM, with 5 Device CALs |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * 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** | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   + zdalny dostęp do graficznego interfejsu Web karty zarządzającej   + 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, SNMP, IPMI2.0, VLAN tagging, SSH   + możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer   + integracja z Active Directory   + możliwość obsługi przez ośmiu administratorów jednocześnie   + Wsparcie dla automatycznej rejestracji DNS   + wsparcie dla LLDP   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej   + możliwość podłączenia lokalnego poprzez złącze RS-232.   + możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy.   + Monitorowanie zużycia dysków SSD   + możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,   + Automatyczne zgłaszanie alertów do centrum serwisowego producenta   + Automatyczne update firmware dla wszystkich komponentów serwera   + Możliwość przywrócenia poprzednich wersji firmware   + Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON   + Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych   + Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.   + Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera   + Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej 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 lub WIFI.   Możliwość rozszerzenia funkcjonalności karty o:   * + możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch   + kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania   + Automatyczne odświeżanie certyfikatów SSL   + możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej   + możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień   + możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera   + możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer   + możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe   + monitorowanie przepływu powietrza na bieżąco (w CFM) |
| **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.   + Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin:     - wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze  Vmware do zdefiniowanej polityki poziomu mikrokodów     - wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityka konfiguracji     - z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)     - inwentaryzacja komponentów w serwerze i ich mikrokodów     - historia poboru mocy i temperatury serwera     - zbieranie danych diagnostycznych serwera do paczki serwisowej |
| **Oprogramowanie do monitorowania** | Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wirtualizacji VMware. 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   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, dla duplikatorów, wraz z informacją o zalecanych wersjach oprogramowania * Raporty   + 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,   + 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   + 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 * 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 25-gramowe 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](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Silver, dla kraju, w którym produkt będzie użytkowany, 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, Microsoft Windows Server 2025. |
| **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. |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i 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. * Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * 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 oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |

1. **Licencje do serwera – 1 sztuka**
2. **Architektura/budowa**
   1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 50 Klientów jednocześnie.
   2. Architektura / budowa:
      1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
      2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).
      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.
      4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.
      5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.
   3. Konfiguracja Architektury:
      1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.
      2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.
3. **Wymagania systemowe**
   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. 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.
      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
   3. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11.
   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.
   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).
   6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.
4. **Interfejsy**
   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.
   2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL
   3. System zapewnia integrację z modelem LLM.
5. **Funkcjonalności systemu zarządzania infrastrukturą IT**
   1. Funkcjonalność Klienta
      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.
   2. Funkcjonalność konsoli administracyjnej.
      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.
      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.
      3. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.
   3. Funkcjonalność panelu pracownika
      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. Zarządzanie licencjami
      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.
   5. Wzorce aplikacji i pakietów
      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.
   6. Inwentaryzacja sprzętu komputerowego i urządzeń.
      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.
   7. Inwentaryzacja urządzeń sieciowych.
      1. System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.
   8. Inwentaryzacja sprzętu.
      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.
   9. Ochrona danych (DLP)
      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
      2. Ochrona danych w ruchu (DR)
         1. Monitorowanie danych przesyłanych za pomocą poczty e-mail oraz blokowanie przesyłania plików określonych typów.
         2. Monitorowanie danych przesyłanych do chmury oraz blokowanie synchronizacji plików określonych typów z wybraną chmurą.
         3. Monitorowania i blokowania operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach.
      3. Klasyfikacja i ochrona dokumentów (KD)
         1. Oznaczanie na dowolnym komputerze (znakowanie przez agenta) określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami.
         2. Znakowanie określonych plików przechowywanych w zasobach serwerów lub udostępnionych zasobach (np. samodzielna macierz dyskowa) wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami, z wykorzystaniem harmonogramu.
   10. Zdalna administracja komputerami
       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.
   11. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.
   12. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.
   13. Zdalne Zarządzanie Zaporą (Firewall)
       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.
   14. Automatyzacja
       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.
   15. Zarządzanie magazynem IT
       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.
   16. Repozytorium
       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.
   17. Kody kreskowe
       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.
   18. Wysyłanie wiadomości
       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.
   19. System musi posiadać możliwość eksportu / importu treści.
   20. Monitorowanie drukarek sieciowych i wydruków
       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.
   21. Monitorowanie stron www
       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.
   22. Monitorowanie serwerów WWW
       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.
   23. Monitorowanie dziennika zdarzeń
       1. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.
   24. System musi umożliwiać monitorowanie komunikatów Syslog.
   25. Monitorowanie pracy komputerów
       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.
   26. Monitorowanie uprawnień ACL
       1. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami.
   27. Monitorowanie sensorów
       1. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.
   28. Repozytorium CMDB
       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.
   29. Worktime manager
       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.
   30. Raportowanie i eksport danych
       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.
   31. System musi zapewnić interfejs API.
       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.
   32. Powiadomienia
       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.
   33. Bezpieczeństwo
       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.
6. **Wsparcie i pomoc**
   * 1. Pomoc techniczna
        1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.
        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.
        3. Czas trwania usługi SLA wynosi 12 miesięcy od dnia zakupu.
7. **Urządzenia do wykonywania backup – 1 sztuka**

|  |  |
| --- | --- |
| **Funkcjonalność** | **Wymagania minimalne** |
| Procesor | Procesor czterordzeniowy 64-bitowy o taktowaniu nie niższym niż 3.3GHz |
| Obudowa | RACK 19" 2U – wraz z kompletem szyn umożliwiającym zamontowanie w szafie RACK |
| Pamięć RAM | Minimum 8 GB DDR4 ECC  Możliwość rozszerzenia pamięci RAM do 32GB. |
| Liczba zatok na dyski twarde | Minimum 12 |
| Obsługiwane dyski twarde | 3.5" SATA HDD / 2.5" SATA SSD – Hot Swap  Zamawiający wymaga dostarczenia 8 dysków 3.5” SATA HDD o pojemności 12 TB każdy o parametrach nie gorszych niż:  Prędkość obrotowa: 7200 RPM  MTBF: 1 200 000  Obciążenie roczne: 180 TB  Pamięć podręczna: 512 MB  Gwarancja producenta dysku: 3 lata  Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego serwera.  Dyski zgodne z listą kompatybilności producenta oferowanego serwera. |
| Możliwość podłączenia modułu rozszerzającego | Tak |
| Minimalna ilość dysków z opcjonalnymi modułami rozszerzającymi, nie mniej niż: | 24 |
| Porty na karty rozszerzeń | Minimum 1 x Gen3 x8 slot (x4 link) |
| Porty LAN | Wbudowane min. 2 x 1GbE RJ-45, 1 x 10GbE RJ-45 |
| Porty USB 3.2 | Minimum 2 |
| Gniazdo rozszerzenia | Minimum 1 |
| Zasilanie | Redundantny zasilacz o mocy minimalnej 350W |
| Mechanizm szyfrowania sprzętowego | Tak, min AES-NI |
| Wewnętrzny system plików | BTRFS, EXT4 |
| Obsługiwane tryby RAID | JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 lub równoważny |
| Uprawnienia | Uprawnienia listy kontroli dostępu systemu Windows (ACL) |
| Usługa katalogowa | Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/FTP/WebDAV/File Station |
| Bezpieczeństwo | Obsługa WORM (Write Once Read Many - jeden zapis, wiele odczytów) dla folderów współdzielonych i migawek, zapora sieciowa, szyfrowanie folderu współdzielonego, szyfrowanie całego woluminu, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów HTTP, HTTPS, SMB, SSH, Telnet, rsync, FTP, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania), dwuetapowa weryfikacja logowania (2FA), adaptacyjna metoda logowania dla konta administratora (AMFA), możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2, U2F, grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail. |
| Oprogramowanie do kopii zapasowej | Oferowany serwer powinien mieć oprogramowanie do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów.  Minimalne wymagane funkcje oprogramowania do backupu:  - kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal,  - kopia zapasowa środowisk MacOS  - kopia zapasowa maszyn wirtualnych (VMware, Hyper-V)  - kopia zapasowa serwerów fizycznych (Windows, Linux)  - obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania,  - obsługa wielu wersji i retencji,  - możliwość wyzwalania kopii zapasowej według harmonogramu,  - obsługa klastra przełączania awaryjnego Microsoft Hyper-V,  - automatyczna weryfikacja utworzonych kopii zapasowych maszyn wirtualnych i serwerów fizycznych, za pomocą utworzonego nagrania wideo z odtworzenia w formie maszyny wirtualnej, - centralne zarządzanie,  - konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji, harmonogramu i woluminów objętych backupem dla poszczególnych zadań,  - portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora),  - delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla użytkowników bez uprawnień administratora,  - kopia zapasowa usług chmur publicznych Microsoft 365 i Google Workspace  Zgodność współpracy oprogramowania do kopii zapasowej z oferowanym serwerem, potwierdzona przez producenta serwera. |
| Oprogramowanie | * Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych * Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników. * Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych serwerów, bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego. Możliwość utworzenia klastra bez konieczności przywracania systemu do ustawień fabrycznych w serwerze aktywnym. * Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych i serwera rsync * Obsługa minimum 256 migawek na folder współdzielony i minimum 4096 migawek na cały system * Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 12jednoczesnych połączeń |
| Gwarancja producenta serwera | Minimum 3 lata  Minimum 1 rok dla szyn montażowych |

1. **Switch – 1 sztuka**

**Wymagania minimalne:**

**Cechy zarządzania**

Typ przełącznika **- Zarządzany**

Warstwa przełącznika **- L3**

Zarządzanie przez stronę www - **Tak**

Obsługa jakość serwisu (QoS)  - **Tak**

Zarządzany w chmurze - **Nie**

**Porty i interfejsy**

Podstawowe przełączanie RJ-45 Liczba portów Ethernet  - **48**

Podstawowe przełączania Ethernet RJ-45 porty typ **- Gigabit Ethernet (10/100/1000)**

Złącze zasilania **- DC-in jack**

Ilość slotów Modułu SFP+  - **4**

Ilość slotów Modułu SFP  **- 4**

Obsługa **10G**

1. **Zasilacz UPS – 1 sztuka**

Zasilacz awaryjny o mocy 15kVA/15kW do zabezpieczenia serwerowni.

UPS 15kVA wykonanyw topologii online VFI-SS-111 (podwójne przetwarzanie) z kompletem baterii 12V o minimalnej pojemności 8,8Ah (40szt) umożliwiającej podtrzymanie pracy dla pełnego obciążenia na czas nie krótszy niż 8 minut. Baterie umieszczone w UPS.

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Nazwa komponentu** | **Parametry techniczne** |
| 1. | Topologia | online, VFI-SS-111, |
| 2. | Moc wyjściowa | 15kVA/15kW; PF=1 |
| 3. | Obudowa | Tower |
| 4. | Zakres napięcia wejściowego | 304 ÷ 478 V AC ± 2% |
| 5. | Napięcie znamionowe (wartość skuteczna) | 3 x 400 V AC |
| 6. | Prąd znamionowy wejście | 28 A |
| 7. | Częstotliwość znamionowa napięcia wejściowego | 50 / 60 Hz |
| 8. | Zakres częstotliwości i tolerancja | 40 ÷ 70 Hz ± 1 Hz |
| 9. | Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa, praca rezerwowa | 380 /400/ 415 V AC ± 1,5% |
| 10. | Prąd znamionowy wyjście | 23 A |
| 11. | Zakres częstotliwości (tolerancja) – praca rezerwowa | 50 / 60 ± 0,1% |
| 12. | Współczynnik odkształceń napięcia wyjściowego THDu | < 5% (nieliniowe wg PN-EN 62040-3) |
| 13. | Współczynnik szczytu CF | 3:1 |
| 14. | Czas przełączenia na pracę rezerwową | 0 ms |
| 15. | Przeciążalność | 110% - 60 min  125% - 10 min  150% - 1min  >150% - 200 ms |
| 16. | Liczba akumulatorów wewnętrznych | 40 (2x 20) |
| 17. | Wymiary (wys. X szer. X gł.) | Nie więcej niż 716 x 251 x 841 mm |
| 18. | Czas podtrzymania dla obciążenia 15kW | Minimum ~ 8 minut w oparciu o minimum 40zt akumulatorów 12V8,8Ah zamontowanych wewnątrz UPS |
| 19. | Przeciążalność | 105-125% - 10min / 125-150% - 30s / >150% - 500ms |
| 20. | EPO | Wymagane – (NC) / (NO) |
| 21. | Przełącznik BYPASSu ręcznego | tak |
| 22. | Bypass zewnętrzny | Wymagany (odpowiedni do oferowanego zasilacza, w obudowie naściennej), instalacja zostanie przeprowadzona przez serwis producenta |
| 23. | Interfejsy komunikacyjne | RS232, RS485, karta styków bezpotencjałowych,  sieciowa karta zarządzająca SNMP wymagana |
| 24. | Język oprogramowania i menu | polski i angielski do wyboru z poziomu interfejsu użytkownika |
| 25. | Wymagane certyfikaty | CE, ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu; (załączyć dokument) |
| 26. | Oprogramowanie do monitorowania pracy zasilacza UPS | **Tego samego producenta co UPS,** pełne, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów **(potwierdzone oświadczeniem producenta oprogramowania)** |
| 27. | Serwis producenta | wymagany, zlokalizowany na terenie Polski, autoryzacja serwisowa lub oświadczenie producenta - załączyć do oferty |
| 28. | Gwarancja | Minimum 24 miesięcy elektronika, 12miesięcy akumulatory, serwis onsite, czas naprawy 14 dni roboczych |
| 29. | Dokumentacja | Instrukcja w języku polskim; oświadczenie producenta o posiadaniu licencji oraz pełnych praw do oprogramowania do monitorowania pracy UPS |
| 30. | Szkolenie | Przeszkolenie pracownika z zakresu obsługi urządzenia w dniu instalacji. Przedstawienie wykazu obowiązków pracownika w zakresie konserwacji oraz monitoringu urządzenia oraz postępowania na wypadek awarii. |