

Załącznik Nr 2

Szczegółowy opis przedmiotu zamówienia część 1 – serwer z systemem operacyjnym
– 1 szt.

Parametr oraz model oferowanego urządzenia wraz ze wskazaniem dodatkowego wyposażenia	Wymagane minimalne parametry
Obudowa	• Obudowa Rack o wysokości max 2U • 12 wnęk na dyski 3,5" • Obudowa z możliwością wyposażenia w panel LED umieszczony na froncie obudowy pozwalający jednocześnie stwierdzić czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej
Płyta główna	• Płyta główna z możliwością zainstalowania minimum jednego procesora. • Możliwość obsługi procesorów 128 rdzeniowych • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym • Na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych do instalacji pamięci • Płyta główna powinna obsługiwać do min. 3TB pamięci RAM
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych
Procesor	Jeden procesor min. 16-rdzeniowy min. 3.0GHZ, klasy x86 dedykowany do pracy z zaoferowanym serwerem . umożliwiające osiągnięcie wyniku min. 177 w teście SPRCrate2017_int_base w konfiguracji jednoprocessorowej, dostępnym na stronie www.spec.org (do oferty należy załączyć wydruk potwierdzający wymagany wynik)
Pamięć RAM	Dwie pamięci: 64 GB DDR5 RDIMM 5600MT/s
Kontroler RAID	Sprzętowy kontroler dysków posiadający min. 8GB nieulotnej pamięci cache, możliwość konfiguracji poziomów RAID : 0,1,5,6,10,50,60, wsparcie dysków samoszyfrujących
Dyski twarde	Zainstalowane: 4x dysk SATA o pojemności min. 8TB, Hot-Plug Zainstalowane dwa dyski M.2.NVMe SSD o pojemności min. 480GB z możliwością konfiguracji RAID 1 W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym gwarancją, uszkodzony nośnik pozostaje własnością zamawiającego i nie podlega zwrotowi do producenta ani serwisu. Wykonawca zobowiązany jest do zapewnienia realizacji naprawy z pozostawieniem wadliwych nośników u zamawiającego (usługa typu Keep Your Drive)
Gniazda PCI	Min. 3 sloty PCIe

Interfejsy sieciowe/FC/SAS	Minimum dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
Wbudowane porty	4 porty USB w tym min.: 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. 1920x1080
Wentylatory	Redundantne
Zasilanie	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 20x Windows Server 2025 User CALs - Nośnik cd/dvd z plikiem instalacyjnym Windows Server 2025 Standard
Bezpieczeństwo	- Zatrask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardech - Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy 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 włączenia i wyłączenia portów USB na obudowie – bez potrzeby restartu serwera - Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależnie 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 800-147Bi 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 karta zarządzająca posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: • Zdalny dostęp do graficznego interfejsu Web karty zarządzającej • Zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) • Szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika • Możliwość podmontowania zdalnych wirtualnych napędów • Wirtualną konsolę z dostępem do myszy , klawiatury • Wsparcie dla IPv6 • Wsparcie dla SNMP, IPMI2.0, VLAN, tagging, SSH • Możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer • Możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • Integracja z Active Directory • Możliwość obsługi przez dwóch administratorów jednocześnie • Wsparcie dla dynamic DNS • Wsparcie dla LLDP • Wysłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • Możliwość podłączenia lokalnego przez złącze RS-232 • Możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy • Monitorowanie zużycia dysków SSD • Możliwość monitorowania z jednej konsoli min. 50 serwerami fizycznymi • Automatyczne zgłaszanie alertów do centrum serwisowego producenta • Automatyczne update firmware dla wszystkich komputerów serwera • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu/ importu konfiguracji (ustawienie karty zarządzającej, BIOS-u, 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 • Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp poprzez urządzenia mobilne – serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji
--------------------------	---

	mobilnej min. (Android/ AppleiOS) przy użyciu jednego z produktów 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 • Kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania • Automatyczne odświeżanie certyfikatów SSL • Możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wieloskładnikowego przy logowaniu do karty zarządzającej • 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 agregata • Wsparcie dla protokołów SNMP, IPMI • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, XLS, PDF • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia • Generowanie alertów przy zmianie stanu urządzenia • Filtry raportów umożliwiające przegląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Kreator umożliwiający dostosowanie akcji do wybranych alertów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • 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 wygenerowania 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 • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności • Zdalne uruchamianie diagnostyki serwera
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wizualizacji Vmware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Ilość podłączonych orz rozłączonych systemów • Stan podłączonych urządzeń • Informację 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 posiadanie oprogramowanie rozszerzające funkcjonalność urządzeń • Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych • Monitorowanie wydajności przepustowości oraz opóźnień dla systemów pamięci masowych • Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersach firmware poszczególnych komponentów adresacji IP karty zarządzającej • Monitoring parametrów z informacją o minimum: - Obciążeniu serwera - Zużyciu pamięci RAM - Temperaturze procesów - Temperaturze powietrza wlotowego - Zużyciu prądu - Zmianach w fizycznej konfiguracji serwera • Monitoring parametrów pamięci masowych z informacją o minimum: - Opóźnieniach - IOPS - Przepustowości - Utylizacji kontrolerów - Pojemności całkowitej i dostępnej 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 reedukacji danych

Informacje o statusie replikacji oraz snapshotów

- Monitoring parametrów przełączników sieciowych z informacją o minimum:

Modelu, oprogramowania, adresaci IP, MAC adres, nr seryjny

Stanie komponentów : zasilacze wentylatory

Podłącznych hostach

Ilości i statusu portów

Utylizacji procesora

Utylizacji poszczególnych portów

Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dla historyczne oraz automatycznie generowana informacja o anomaliach

- Aktualizacja firmware

Możliwość aktualizacji firmaware, oprogramowania zarządzającego dla systemów pamięci masowej, serwerów, rozwiązań HCI, systemów przełączników FC, 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

- Możliwości generowania raportów dla systemów pamięci masowych zawierających informację o:

Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji programowania, zajętości systemu oraz poziomu redukcji danych, informacji o utworzonych LUN-ach i systemach pliku, status replikacji

- Generowania 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 dostarczone w ramach postępowania - Posiadane przez zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI Wirtualny asystent - Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizę 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 - Oferowana platforma musi posiadać dedykowaną aplikację na urządzenie iOS oraz Android
Certyfikaty	- Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 - Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami - Serwer musi posiadać deklarację CE - 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 elektryczne oraz niebezpieczne składniki powinny być bezpieczne i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy EEE2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użycia/ zdalnych 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 potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku – wykonawca złoży dokument potwierdzający spełnienie wymogu - Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Serwer 2022, Microsoft Windows Serwer 2025
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim

	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela
Warunki gwarancji	- Okres gwarancji minimum 60 miesięcy - Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 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 sprawy - Certyfikowany pracownik producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym od zakończenia diagnostyki - Naprawa ma się odbyć w siedzibie zamawiającego, chyba że zamawiający dla danej naprawy zgłosi inną formę - Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: wykrywanie usterek sprzętowych, 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 oświadczenie, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym , uszkodzony dysk pozostaje u zamawiającego