Załącznik nr 1

**Szczegółowy Opis Przedmiotu Zamówienia**

Dostawa sprzętu komputerowego, oprogramowania i urządzeń sieciowych wraz z wdrożeniem w ramach kompleksowej modernizacji infrastruktury informatycznej i systemu cyberbezpieczeństwa

Rudna Mała, grudzień 2025

Spis treści

[1 Wymagania ogólne dla urządzeń i oprogramowania sieciowego. 4](#_Toc218007273)

[2 Miejsce instalacji sprzętu i oprogramowania/systemu: 5](#_Toc218007274)

[3 Zakres wymaganych dostaw 5](#_Toc218007275)

[4 Szczegółowy opis pozycji 8](#_Toc218007276)

[4.1 Platforma wirtualizacyjna (środowiska bez baz danych Oracle) 8](#_Toc218007277)

[4.1.1 Serwer v1 4 szt. 8](#_Toc218007278)

[4.1.2 Licencja na serwerowy system operacyjny 1 szt. 13](#_Toc218007279)

[4.1.3 Licencja dostępowa do systemu operacyjnego 1 szt. 18](#_Toc218007280)

[4.2 Platforma wirtualizacyjna (środowiska z bazami danych Oracle) 19](#_Toc218007281)

[4.2.1 Serwer v2 2 szt. 19](#_Toc218007282)

[4.2.2 Wsparcie dla systemu Oracle Linux 25](#_Toc218007283)

[4.3 Zasoby dyskowe dla środowisk wirtualnych 25](#_Toc218007284)

[4.3.1 Macierz dyskowa 2 szt. 25](#_Toc218007285)

[4.3.2 Przełącznik sieciowy SAN 2 szt. 31](#_Toc218007286)

[4.3.3 Wkładki FC32Gb short wave 28 szt. 33](#_Toc218007287)

[4.3.4 Wkładki FC32Gb long wave 4 szt. 33](#_Toc218007288)

[4.4 LAN – urządzenia sieciowe 33](#_Toc218007289)

[4.4.1 Przełącznik sieciowy v1 4 szt. 33](#_Toc218007290)

[4.4.2 Przełącznik sieciowy v2 11 szt. 35](#_Toc218007291)

[4.4.3 Przełącznik sieciowy v3 11 szt. 37](#_Toc218007292)

[4.4.4 Przełącznik sieciowy v4 4 szt. 39](#_Toc218007293)

[4.5 Zestawy komputerowe 41](#_Toc218007294)

[4.5.1 Komputer typu All-in-One 176 szt. 41](#_Toc218007295)

[4.5.2 Komputer stacjonarny 13 szt. 50](#_Toc218007296)

[4.5.3 Pakiet biurowy 189 szt. 58](#_Toc218007297)

[4.6 Backup danych 62](#_Toc218007298)

[4.6.1 Urządzenie do przechowywania i deduplikacji danych 1 szt. 62](#_Toc218007299)

[4.6.2 Serwer backupu 1 szt. 71](#_Toc218007300)

[4.6.3 Oprogramowania backupu danych 1 szt. 77](#_Toc218007301)

[4.7 Cyberbezpieczeństwo 88](#_Toc218007302)

[4.7.1 Urządzenie UTM v1 2 szt. 88](#_Toc218007303)

[4.7.2 Urządzenie UTM v2 2 szt. 97](#_Toc218007304)

[4.7.3 Oprogramowanie do zbierania oraz analizy logów sieciowych 1 szt. 107](#_Toc218007305)

[4.8 Licencja na oprogramowanie antywirusowe 110](#_Toc218007306)

[4.9 Urządzenia sieci bezprzewodowej 111](#_Toc218007307)

[4.9.1 Punkt dostępowy WLAN 50 szt. 111](#_Toc218007308)

[4.9.2 Licencja na system uwierzytelniania, autoryzacji i kontroli dostępu 1 szt. 112](#_Toc218007309)

[4.10 Modernizacja sieci LAN 117](#_Toc218007310)

[4.11 Wdrożenie 118](#_Toc218007311)

# Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

* całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim;
* całość sprzętu musi być fabrycznie nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana wcześniej;
* wszystkie dostarczone i montowane komponenty przez Wykonawcę muszą być dopuszczone do obrotu na terenie Unii Europejskiej;
* dostarczane urządzenia muszą być pozbawione wszelkich wad;
* urządzenia muszą być kompletne i gotowe do pracy po podłączeniu
* wszystkie oferowane urządzenia w ramach poszczególnych typów musza być:
* złożone z identycznych podzespołów, sygnowanych przez ich Producenta;
* dostarczane w oryginalnych opakowaniach Producenta (opakowania nie mogą być otwierane od momentu wyprodukowania przez Producenta do momentu dostawy do Zamawiającego, fabryczne zamknięcie fabrycznych opakowań).
* gwarancja dostawy sprzętu tego samego modelu/serii przez cały okres trwania projektu.

**Sprzęt**

* serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
* Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Wnioskodawcy), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
* Gwarantowany czas naprawy nie może być dłuższy niż 10 dni roboczych. W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
* Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Wnioskodawcy;
* wszystkie dostarczane moduły muszą pochodzić od producenta urządzeń sieciowych i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu (Zamawiający dopuszcza zastosowanie zamienników dla wkładek do przełączników opisanych w punkcie 4.8 i 4.9 – wkładki musza spełniać normy jakościowe i technologiczne);
* **Postanowienia dotyczące nośników danych (dysków):**
* W przypadku awarii, uszkodzenia lub wymiany dysku twardego (HDD/SSD) wchodzącego w skład dostarczonego sprzętu:
  + Uszkodzony dysk pozostaje u Zamawiającego i nie podlega zwrotowi Wykonawcy ani producentowi.
  + Wykonawca zobowiązany jest do dostarczenia nowego, sprawnego dysku w miejsce uszkodzonego, bez dodatkowych kosztów dla Zamawiającego (w ramach gwarancji/serwisu).
* Zapis ten ma na celu zapewnienie bezpieczeństwa danych przechowywanych na nośnikach, niezależnie od ich stanu technicznego.
* Wykonawca uwzględnia powyższe postanowienia przy kalkulacji ceny oferty oraz przy realizacji usług serwisowych.
* Zamawiający zastrzega sobie prawo do samodzielnego zniszczenia lub utylizacji uszkodzonych nośników zgodnie z obowiązującymi procedurami bezpieczeństwa i ochrony danych.

**Oprogramowanie**

* oprogramowanie powinno posiadać min 36-miesięczną gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba że zapisy szczegółowe stanowią inaczej);
* gwarancja nie obejmuje kosztów bieżącego utrzymania (opieka serwisowa, upgrade systemów, wersji, prawa do aktualizacji) wdrożonego oprogramowania po okresie realizacji projektu.

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części SOPZ.

**Równoważność**

„Zamawiający wyjaśnia, że ilekroć w Opisie Przedmiotu Zamówienia (OPZ) wskazano znaki towarowe, patenty lub pochodzenie (np. *Microsoft Hyper-V, Oracle Linux Virtualization Manager, Commvault, Veeam*), należy je traktować jako przykładowe, mające na celu doprecyzowanie standardu technicznego i funkcjonalnego. Zamawiający, zgodnie z Zasadą Konkurencyjności, dopuszcza rozwiązania równoważne.

Przez **rozwiązanie równoważne** w zakresie kluczowych systemów Zamawiający rozumie rozwiązania spełniające łącznie następujące minimalne kryteria techniczne i licencjonowania:

1. **W zakresie Platformy Wirtualizacyjnej dla środowiska Oracle (zamiast Oracle Linux Virtualization Manager):** Ze względu na posiadany model licencjonowania baz danych Oracle (Processor Metric), rozwiązanie równoważne musi:

* Posiadać mechanizm **Hard Partitioning** (twarde partycjonowanie zasobów CPU) uznawany i certyfikowany przez firmę Oracle, pozwalający na ograniczenie liczby wymaganych licencji bazodanowych wyłącznie do rdzeni przypisanych maszynie wirtualnej, a nie całego serwera fizycznego.
* *Uzasadnienie:* Zaoferowanie rozwiązania niespełniającego tego wymogu (np. standardowy soft-partitioning) naraziłoby Zamawiającego na wielomilionowe koszty dodatkowych licencji bazodanowych, co stanowiłoby nienależyte wykonanie zamówienia.
* Zapewniać pełne wsparcie techniczne producenta (Vendor Support) dla systemów operacyjnych Oracle Linux w modelu 24/7.

1. **W zakresie Platformy Wirtualizacyjnej Ogólnego Przeznaczenia (zamiast Microsoft Hyper-V):** Rozwiązanie równoważne musi:

* Zapewniać pełną kompatybilność z posiadanym przez Zamawiającego systemem centralnego zarządzania oraz usługami katalogowymi (Active Directory), bez konieczności zakupu dodatkowych konektorów (connectors) czy bramek (gateways).
* Umożliwiać migrację maszyn wirtualnych z obecnego środowiska bez konieczności długotrwałego przestoju (akceptowalny czas przełączenia tożsamy z wymaganym dla Hyper-V).
* Zapewniać obsługę funkcji *Secure Boot* dla systemów gości Windows Server w sposób zgodny z wymogami cyberbezpieczeństwa określonymi w OPZ.

1. **W zakresie Systemu Backupu (zamiast Commvault/Veeam):** Rozwiązanie równoważne musi:

* Posiadać natywne wsparcie (bez stosowania skryptów zewnętrznych) dla deduplikacji "na źródle" (source-side deduplication) kompatybilnej z oferowanym sprzętowym urządzeniem do deduplikacji.
* Obsługiwać mechanizm wykonywania kopii zapasowych spójnych z aplikacją (application-aware) dla posiadanych przez Zamawiającego systemów: MS SQL, Oracle RAC, Active Directory.
* Gwarantować, że zmiana oprogramowania nie wymusi na Zamawiającym zakupu nowych licencji na systemy operacyjne lub bazy danych w celu instalacji agentów backupu.”

# Miejsce instalacji sprzętu i oprogramowania/systemu:

* Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części załącznika na 1 do SIWZ, w budynkach szpitala w miejscach wskazanych przez Zamawiającego.
* W przypadku komputerów Zamawiający wymaga dostaw częściowych (po 50-100 szt.), odbywających się partiami w ustalonym harmonogramie dostaw. Wykonawca musi w ofercie przewidzieć magazynowanie komputerów oraz dostawy częściowe.

# Zakres wymaganych dostaw

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa pozycji** | **Ilość** | **Wymagania gwarancyjne i serwisowe** |
| **4.1** | **Platforma wirtualizacyjna (bez Oracle)** |  |  |
| 1. | Serwer v1 | 4 szt. | **36 miesięcy** gwarancji producenta. Zgłoszenia 24/7/365. Naprawa **NBD** (następny dzień roboczy) w miejscu instalacji. **Zachowanie dysku twardego** u Zamawiającego w przypadku awarii. |
| 2. | Licencja na serwerowy system operacyjny | 1 szt. | Zgodnie z zasadami licencjonowania. |
| 3. | Licencja dostępowa (300 szt.) | 1 szt. | Zgodnie z zasadami licencjonowania producenta |
| **4.2** | **Platforma wirtualizacyjna (z Oracle)** |  |  |
| 4. | Serwer v2 | 2 szt. | **36 miesięcy** gwarancji producenta. Zgłoszenia 24/7/365. Naprawa **NBD** w miejscu instalacji. **Zachowanie dysku twardego** u Zamawiającego. |
| 5. | Wsparcie dla systemu Oracle Linux | 2 szt. | Wsparcie producenta typu **Premier Support na 3 lata**. |
| **4.3** | **Zasoby dyskowe** |  |  |
| 6. | Macierz dyskowa | 2 szt. | **36 miesięcy** gwarancji producenta. Zgłoszenia 24/7/365. Naprawa **NBD** w miejscu instalacji. **Zachowanie dysku twardego** u Zamawiającego. |
| 7. | Przełącznik sieciowy SAN | 2 szt. | **36 miesięcy** gwarancji producenta. Zgłoszenia 24/7/365. Naprawa **NBD** w miejscu instalacji. |
| 8. | Wkładki FC32Gb short wave | 28 szt. | Objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu (min. 3 lata zgodnie z wymogami ogólnymi). |
| 9. | Wkładki FC32Gb long wave | 4 szt. | Objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu (min. 3 lata zgodnie z wymogami ogólnymi). |
| **4.4** | **LAN – urządzenia sieciowe** |  |  |
| 10. | Przełącznik sieciowy v1 | 4 szt. | Min. **3 lata** gwarancji (wymogi ogólne). Funkcje dostępne permanentnie (brak licencji czasowych). |
| 11. | Przełącznik sieciowy v2 | 11 szt. | Min. **3 lata** gwarancji (wymogi ogólne). Funkcje dostępne permanentnie. |
| 12. | Przełącznik sieciowy v3 | 11 szt. | Min. **3 lata** gwarancji (wymogi ogólne). Funkcje dostępne permanentnie. |
| 13. | Przełącznik sieciowy v4 | 4 szt. | **3 lata** gwarancji producenta. Zgłoszenia 365x7x24. Naprawa **NBD** w miejscu instalacji. |
| **4.5** | **Zestawy komputerowe** |  |  |
| 14. | Komputer typu All-in-One | 176 szt. | Min. **3 lata** gwarancji producenta. Naprawa **NBD** w miejscu instalacji. **Zachowanie dysku twardego** u Zamawiającego. |
| 15. | Komputer stacjonarny | 13 szt. | Min. **3 lata** gwarancji producenta. Naprawa **NBD** w miejscu instalacji. **Zachowanie dysku twardego** u Zamawiającego. |
| 16. | Pakiet biurowy | 189 szt. | Licencja wieczysta. Zgodnie z zasadami licencjonowania producenta. |
| **4.6** | **Backup danych** |  |  |
| 17. | Urządzenie do deduplikacji | 1 szt. | Min. **3 lata** gwarancji producenta. Zgłoszenia 24/7/365. Naprawa **NBD** w miejscu instalacji. **Zachowanie dysku twardego** u Zamawiającego. |
| 18. | Serwer backupu | 1 szt. | **Min. 36 miesięcy** gwarancji producenta. Zgłoszenia 24/7/365. Naprawa **NBD** w miejscu instalacji. **Zachowanie dysku twardego** u Zamawiającego. |
| 19. | Oprogramowanie backupu | 1 szt. | Subskrypcja na **3 lata**. Zgodnie z zasadami licencjonowania producenta. |
| **4.7** | **Cyberbezpieczeństwo** |  |  |
| 20. | Urządzenie UTM v1 | 2 szt. | Serwis gwarancyjny producenta przez **36 miesięcy**. Wsparcie 24x7, dostęp do aktualizacji. |
| 21. | Urządzenie UTM v2 | 2 szt. | Serwis gwarancyjny producenta przez **36 miesięcy**. Wsparcie 24x7, dostęp do aktualizacji. |
| 22. | System analizy logów | 1 szt. | Serwis producenta przez **36 miesięcy**. Wsparcie 24x7, dostęp do aktualizacji. Licencja "na własność" (niewykupienie wsparcia nie blokuje systemu). |
| **4.8** | **Antywirus** |  |  |
| 23. | Licencja antywirusowa | 1 kpl. | Rozszerzenie ważności licencji o **36 miesięcy** od daty zakończenia obecnej. |
| **4.9** | **Sieć bezprzewodowa** |  |  |
| 24. | Punkt dostępowy WLAN | 50 szt. | **Dożywotnia ograniczona gwarancja** (do 5 lat od końca produkcji). Serwis producenta przez min. **36 miesięcy** (naprawa/wymiana, wsparcie 24x7). |
| 25. | Licencja (NAC) | 1 szt. | Serwis producenta przez **36 miesięcy** (aktualizacje + wsparcie 24x7). |
| **4.10** | **Modernizacja sieci LAN** | **1 szt.** |  |
| **4.11** | **Wdrożenie** | **1 szt.** |  |

# Szczegółowy opis pozycji

## Platforma wirtualizacyjna (środowiska bez baz danych Oracle)

### Serwer v1 4 szt.

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| **Obudowa** | Obudowa Rack o wysokości max. 2U z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych z organizerem do kabli.  Możliwość zainstalowania karty umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne  - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | Zainstalowane dwa procesory 16-rdzeniowe klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 388 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. Dla oferowanego serwera. |
| **RAM** | Min. 512GB DDR5 RDIMM 6400MT/s w kościach min. 32GB. Na płycie głównej powinno znajdować się minimum 32 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM. |
| **Zabezpieczenia pamięci RAM** | Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection |
| **Gniazda PCIe** | - minimum cztery sloty PCIe x16 generacji 5 oraz minimum dwa sloty OCP 3.0. |
| **Interfejsy sieciowe/FC/SAS** | Jedna dwuportowa karta sieciowa 25Gb Ethernet ze złączami SFP28 nie zajmująca slotów PCIe.  Dodatkowo zainstalowane:  - jedna karta dwuportowa FC 32Gb/s |
| **Dyski twarde** | Zainstalowane dwa dyski hot-swap M.2 NVMe o pojemności min. 480GB z możliwością konfiguracji RAID 1. |
| **Wbudowane porty** | min. port USB 2.0 oraz dwa porty USB 3.1, port VGA, |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900 |
| **Wentylatory** | Redundantne Hot-Plug |
| **Zasilacze** | Min. dwa zasilacze Hot-Plug min. 1500W Titanium. |
| **Bezpieczeństwo** | Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.  Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą  TPM 2.0  Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera  Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.  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. |
| **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 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 za pomocą interfejsu USB-C na froncie serwera, który pozwala na bezpośredni dostęp interfejsu karty zarządzającej (zarówno UI w przeglądarce, jak i konsolę RACADM czy API Redfish) bez potrzeby połączenia sieciowego * Monitorowanie zużycia dysków SSD * 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 opraciu 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. * 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 wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych |
| **Oprogramowanie do zarządzania** | Możliwość zainstalowania oprogramowania producenta serwera do zarządzania, spełniające 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 opraciu o wszystkie informacje zawarte w inwentarzu. * Grupowanie urządzeń w oparciu o kryteria użytkownika * Tworzenie automatycznie grup urządzeń w opraciu 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 zarzadzającym. * Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| **Normy Środowiskowe** | 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 rozporządzenia nr 1272/2008WE. 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 potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001 lub równoważnymi.  Serwer musi posiadać deklaracja CE.  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub równoważną.  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2022 x64, Microsoft Windows 2025. |
| **Warunki gwarancji** | Zamawiający wymaga min. 36 miesięcy gwarancji producenta możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365  następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.  Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej  (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik ***producenta*** z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu. |
| **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. |

### Licencja na serwerowy system operacyjny 1 szt.

|  |
| --- |
| Licencja musi obejmować 128 rdzeni procesorów klastra czterech serwerów opisanych w p.4.1.1 niniejszej specyfikacji.  Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym klastra złożonego z 4 serwerów i nielimitowanej liczby wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:   * Możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym. * Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny. * Możliwość budowania klastrów składających się z 64 węzłów. * Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu. * Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. * Ochrona firmware przed atakami poprzez izolację hypervisora technologią Dynamic Root of Trust of Measurement (DRTM). * Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. * Wbudowane wsparcie instalacji i pracy na wolumenach, które:   + pozwalają na zmianę rozmiaru w czasie pracy systemu,   + umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,   + umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,   + umożliwiają zdefiniowanie list kontroli dostępu (ACL). * Wbudowany asystent aktualizacji obejmujący możliwość upgrade z trzech ostatnich wersji systemu. * Narzędzie wiersza poleceń, które umożliwia użytkownikom monitorowanie i rozwiązywanie problemów z wydajnością systemu w czasie rzeczywistym, pozwalające dynamicznie instrumentować zarówno jądro, jak i kod w przestrzeni użytkownika bez konieczności modyfikowania samego kodu. * Wbudowana możliwość zakładania kont w systemie:   + Microsoft Entra ID   + Microsoft account   + Work or school account. * Rozbudowane schematy Active Directory obejmujące sch89.ldf, sch90.ldf i sch91.ldf. * Poziom funkcjonalności domeny i lasu dostosowany rozmiaru strony bazy danych 32k, odwzorowywany na wartość DomainLevel 10 i ForestLevel 10 dla instalacji nienadzorowanych. * Wystąpienia kontrolerów domeny i usług LDS w usłudze AD zezwalają protokołowi LDAP na dodawanie, wyszukiwanie i modyfikowanie operacji obejmujących atrybuty poufne tylko wtedy, gdy połączenie jest szyfrowane.   Narzędzia wspierające tworzenie klastra hiperkonwergentnego (łączącego magazyn i zasoby obliczeniowe w węzłach klastra).   * Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. * Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. * Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET * Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. * Możliwość wykorzystania standardu http/2. * Wbudowana obsługa TLS 1.3 włączona jako ustawienie standardowe. * Możliwość przechowywania wrażliwych danych i kluczy pod ochroną TPM 2.0. * Izolacja kernela od pozostałych komponentów systemu w oparciu zabezpieczenia bazujące na wirtualizacji (VBS) chroniąca przed metodami ataków wykorzystujących podatności używane przy „kopaniu” kryptowalut. * Dostępność usługi DNS-over-HTTPS (DoH) szyfrujących zapytania DNS przy użyciu HTTPS. * Dostępność usługi Server Message Block (SMB) z szyfrowaniem AES-256 (AES-256-GCM and AES-256-CCM), automatycznie wykorzystywanych przy połączeniach z urządzeniami wspierającymi te metody. * Szyfrowanie komunikacji i wspólnych zasobów wewnątrz klastra niezawodnościowego. * Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. * Wsparcie dla technologii Azure Arc pozwalające na traktowanie serwera zainstalowanego we własnym centrum przetwarzania jako zarządzalnego zasobu Azure. * Dostępne dwa rodzaje graficznego interfejsu użytkownika: * Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, * Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. * Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, * Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. * Mechanizmy logowania w oparciu o: * Login i hasło, * Karty z certyfikatami (smartcard), * Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), * PIN zdefiniowany dla urządzenia, * Rozpoznawanie twarzy. * Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. * Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). * Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. * Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. * Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). * Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. * Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: * Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, * Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:   Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.   * Zdalna dystrybucja oprogramowania na stacje robocze. * Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników. * Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:   Dystrybucję certyfikatów poprzez http  Konsolidację CA dla wielu lasów domeny,  Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.   * Szyfrowanie plików i folderów. * Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). * Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi. * Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. * Serwis udostępniania stron WWW. * Wsparcie dla protokołu IP w wersji 6 (IPv6), * Wsparcie dla algorytmów Suite B (RFC 4869), * Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, * Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. * Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. * Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. * Mechanizmy wirtualizacji mające wsparcie dla:   Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  Obsługi 4-KB sektorów dysków  Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)  Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.   * Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów. * Wsparcie dla rozwiązania dla rozwiązań kontenerowych dla aplikacji zgodnych z Kubernetes. * Możliwość wykorzystywania aplikacji kontenerowych wymagających wykorzystania Azure Active Directory bez dołączania hosta kontenerów do domeny. * Wsparcie migracji zasobów na dyskach do Azure. * Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. * Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). * Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB. * Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. * Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. * Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. * Mechanizm konfiguracji połączenia VPN do platformy Azure. * Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu. * Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów. * Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. |

### Licencja dostępowa do systemu operacyjnego 1 szt.

|  |
| --- |
| Licencja dostępowa typu Device do systemu operacyjnego z p. 4.1.2 niniejszej specyfikacji, w ilości 300 szt. |

## Platforma wirtualizacyjna (środowiska z bazami danych Oracle)

### Serwer v2 2 szt.

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| **Obudowa** | Obudowa Rack o wysokości max 2U z kompletem szyn umożliwiających montaż w szafie rack wraz organizerem do kabli. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych. |
| **Procesor** | Zainstalowany jeden procesor min. 24-rdzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 384 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org. |
| **RAM** | Min. 512GB DDR5 RDIMM 6400MT/s, na płycie głównej powinno znajdować się minimum 24 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 6TB pamięci RAM. |
| **Gniazda PCIe** | Minimum sześć slotów PCIe x16 Gen5  Dodatkowo min. jeden slot OCP 3.0 |
| **Interfejsy sieciowe/FC** | Jedna karta dwuportowe 25Gb Ethernet w standardzie SFP28 nie zajmująca slotów PCIe.  Dodatkowo zainstalowane:  - Jedna karta dwuportowa FC 32Gb/s |
| **Napęd optyczny** | Nie wymagany |
| **Dyski twarde** | Zainstalowane dwa dyski M.2 NVMe hot-plug o pojemności min. 480GB, możliwość skonfigurowania RAID 1. |
| **Wbudowane porty** | min. 1 port USB 2.0 oraz 2 porty USB 3.1, 1 port VGA |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200. |
| **Wentylatory** | Redundantne hot-plug |
| **Zasilacze** | Redundantne, Hot-Plug min. 1500W Titanium |
| **Bezpieczeństwo** | Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.  Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą  TPM 2.0  Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera  Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.  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. |
| **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 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 za pomocą interfejsu USB-C na froncie serwera, który pozwala na bezpośredni dostęp interfejsu karty zarządzającej (zarówno UI w przeglądarce, jak i konsolę RACADM czy API Redfish) bez potrzeby połączenia sieciowego * Monitorowanie zużycia dysków SSD * 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 opraciu 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. * komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI. * 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 wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych * Musi oferować wbudowany dziennik cyklu życia sprzętu, który rejestruje szczegółowe zdarzenia dotyczące konfiguracji, integracji fizycznych i operacji serwera, powiązane bezpośrednio z tożsamością użytkownika inicującego zmiany, umożliwiając pełną audytowalność od momentu produkcji do użytkowania. |
| **Oprogramowanie do zarządzania** | Możliwość instalacji oprogramowania producenta do zarządzania, spełniające 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 opraciu 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. |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001 lub normami równoważnymi.  Serwer musi posiadać deklaracja CE. 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. |
| **Normy Środowiskowe** | 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 potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku***.***      Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. |
| Warunki gwarancji | Zamawiający wymaga min. 36 miesięcy gwarancji producenta możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365  następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.  Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej  (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik ***producenta*** z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym od otrzymania zakończenia diagnostyki. Naprawa ma się odbywać 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  Zamawiający wymaga, aby w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostał u Zamawiającego.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu. |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. |

### Wsparcie dla systemu Oracle Linux

|  |
| --- |
| Wsparcie Oracle Linux Premier Support/Physical CPU Pair/3 lata 2 szt. |

## Zasoby dyskowe dla środowisk wirtualnych

### Macierz dyskowa 2 szt.

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| **Obudowa** | Obudowa typu Rack 19” – musi być dostarczona wraz z szynami do instalacji w szafie umożliwiającymi jej serwisowanie.  Macierz musi być wyposażona w minimum 2 kontrolery  Do urządzenia należy dołączyć kable połączeniowe zgodnie z ilością portów i rodzajem zainstalowanych modułów.  Oferowane rozwiązanie musi zawierać się w obudowie o maksymalnej wysokości 2U |
| **Skalowalność** | Macierz musi umożliwiać skalowalną rozbudowę on-line Scale-out do minimum 8 kontrolerów zarządzanych z jednej konsoli i 372 dysków oraz Scale-in poprzez dodawanie półek dyskowych do par kontrolerów. Pojedyncza para kontrolerów musi umożliwiać obsługę minimum 90 dysków NVMe. Po takiej rozbudowie musi być możliwość zaprezentowania każdego wolumenu logicznego LUN przez dowolny z kontrolerów bez przerywania dostępu do danych.  Oferowane rozwiązanie musi mieć możliwość rozbudowy do 360 rdzeni oraz minimum 7TB pamięci RAM. Rozbudowa nie może powodować wymiany zastosowanych dysków twardych ani kontrolerów. |
| **Kontrolery** | Każdy kontroler macierzy musi być wyposażony w co najmniej 96GB przestrzeni cache służącej do buforowania operacji odczytu oraz zapisu.  Kontrolery muszą wspierać jednocześnie ruch - blokowy i plikowy (wymagane protokoły: iSCSI, FC oraz plikowy CIFS - minimum SMB w wersjach 3, 3.1 FTP i SFTP oraz NFS 3, 4, 4,1 4,2). Nie dopuszcza się realizacji funkcjonalności ruchu plikowego za pomocą dodatkowych zewnętrznych urządzeń.  Oferowane rozwiązanie musi obsługiwać protokół NVMe na całej ścieżce komunikacji (front-end, back-end). Nie dopuszcza się stosowanie rozwiązania, w którym rozbudowa o dodatkowe półki dyskowe odbywała się po protokole innym niż NVMe.  Macierz musi natywnie wspierać protokół NVMe-OF w tym NVMe-OF/TCP oraz NVMe-OF/FC.  Kontrolery te muszą działać w sposób redundantny – tj. przy uszkodzeniu dowolnego kontrolera, macierz musi nadal działać i utrzymywać dostęp do odczytu i zapisu danych. Praca w trybie active/active w taki sposób, aby oba kontrolery były aktywne i w tym samym czasie udostępniały urządzenia LUN oraz zasoby plikowe. Oba kontrolery muszą brać czynny udział w obsłudze wszystkich operacji (snapshot, clone, replikacja). Nie dopuszcza się rozwiązania, w którym jeden z kontrolerów działa jedynie jako urządzenie przekazujące ruch do hostów.  Macierz musi być odporna na awarię pamięci cache, w szczególności cache przeznaczony do zapisu (ang. write cache) i zapewniać w razie utraty zasilania zabezpieczenie danych niezapisanych na dyski przez nieograniczony czas.  Każdy kontroler macierzy musi być oparty o jeden wielordzeniowy procesor (minimum 12 rdzeni łącznie) i pracować z częstotliwością minimum 2.2 GHz.  Macierz musi umożliwiać wykonywanie procesu aktualizacji mikrokodu w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji. |
| **Zasilanie** | Urządzenie musi być wyposażone w podwójny, redundantny system zasilania i chłodzenia, gwarantujący nieprzerwany dostęp do wolumenów dyskowych (LUN) oraz działania pamięci cache w przypadku awarii jednego ze źródeł zasilania. Pojedynczy zasilacz nie może przekraczać mocy 1500W. |
| **Przestrzeń dyskowa** | Dostarczona Macierz musi zapewnić przestrzeń efektywną (po zastosowaniu mechanizmów kompresji i deduplikacji) minimum 203TB  Osiągnięta przestrzeń 203TB musi być zapewniona i gwarantowana przez producenta macierzy. Macierz musi posiadać możliwość zapełnienia całej dostarczonej przestrzeni. Jeśli macierz pozwala na zapełnienie tylko części przestrzeni (np. 80%) to pozostająca „pusta- niewykorzystana” przestrzeń nie będzie wliczona w dostarczoną przestrzeń.  Oferowana przestrzeń musi składać się minimum 8 dysków SSD NVMe Hot-Swap o pojemności min. 7.68TB. Nie dopuszcza się stosowania dedykowanych modułów zamiast urządzeń dyskowych SSD z komórkami innymi niż TLC, SCM oraz NVRAM.  Macierz musi umożliwiać instalację minimum 17 dodatkowych dysków NVMe bez dodawania półek, kontrolerów, czy innych elementów.  Oferowana macierz musi umożliwiać rozbudowę z granulacją jednego dysku.  Macierz w dostarczonej konfiguracji (z włączoną deduplikacją i kompresją) musi umożliwiać osiągnięcie wydajności minimum 99 tysięcy IOPS z przestrzeni dyskowej (przy założeniach: dla bloku danych o wielkości 8k odczyt 70%, zapis 30% oraz wszystkie operacje losowe, 0% trafień w cache)  Macierz w dostarczonej konfiguracji (z włączoną deduplikacją i kompresją) musi umożliwiać osiągnięcie minimum 810 MB/s odczytu z przestrzeni dyskowej (nie z cache macierzy)  W zaproponowanej konfiguracji macierzy należy także zabezpieczyć przestrzeń hot/spare według zaleceń producenta macierzy. Niedopuszczalne jest zastosowanie dedykowany dysków jako dyski hot-spare.  Macierz w żadnej konfiguracji nie może oferować obsługi dysków obrotowych, a co za tym idzie nie może oferować rozbudowy o dyski obrotowe czyli musi być rozwiązaniem zaprojektowanym tylko i wyłącznie do dysków SSD lub modułów flash.  Do oferty należy dołączyć wydruk z narzędzia producenta oferowanej macierzy konfiguratora / estymatora – potwierdzający spełnienie powyższych wymagań (zawierający zarówno proponowaną konfigurację sprzętową z dokładnym wskazaniem part number’ów elementów jak i ich ilości, w tym typów i okresów wsparcia licencji i gwarancji) jak i wynikające z niej parametry pojemnościowe i wydajnościowe) |
| **Redukcja danych** | Rozwiązanie musi zapewniać mechanizm kompresji i deduplikacji danych w trybie in-line. Kompresja i deduplikacja muszą być integralną częścią systemu macierzowego bez możliwości zatrzymania bądź wyłączenia przez administratora. Mechanizmy kompresji i dedpuplikacji muszą być przezroczyste dla administratora macierzy.  Proces deduplikacji musi odbywać się globalnie (minimum w ramach pary kontrolerów).  Wobec powyższych wymagań dla każdego wolumenu macierzy musi zachodzić jednocześnie kompresja i deduplikacja danych, która nie wymaga konfiguracji ani żadnej innej interwencji ze strony administratora macierzy. Operacje kompresji i deduplikacji muszą działać na wszystkich rodzajach dostarczanych i opcjonalnych nośników SSD i być dostępne dla wszystkich rodzajów przechowywanych danych (nie jest dozwolone oferowanie rozwiązań, które nie zapewniłyby kompresji i deduplikacji na całej wymaganej pojemności).  Redukcja danych musi być wspierana przez dedykowany układ sprzętowy poza procesorem kontrolera macierzy.  Mechanizmy redukcji danych muszą być realizowane za pomocą zmiennego bloku, aby zapewnić maksymalną skuteczność tych procesów.  Wymagane jest zagwarantowane przez producenta oferowanej macierzy osiągnięcie współczynnika redukcji danych dla całej macierzy na poziomie 5:1 przy spełnieniu wymagań pojemnościowych określonych w punkcie Przestrzeń dyskowa.  Jeżeli producent nie gwarantuje współczynnika redukcji danych dla całej macierzy na poziomie 5:1 lub gwarantuje je w niższym stopniu, należy dostarczyć taką przestrzeń użyteczną, aby przestrzeń efektywna wynosiła 203TB  W powyższej kalkulacji nie będzie wymagane uwzględnienie danych wcześniej zaszyfrowanych (z pominięciem mechanizmu szyfrowania przez macierz) i wcześniej skompresowanych. |
| **Obsługa dysków** | Macierz dyskowa musi umożliwiać stosowanie w niej na potrzeby składowania danych minimum dysków, SSD NVMe lub NVMe SCM**.** Dyski NVMe SCM muszą być wykorzystywane na przechowywanie danych.  Macierz musi być wyposażona w dyski posiadające podwójne interfejsy. |
| **Porty macierzowe** | Oferowane urządzenie musi być wyposażone w minimum:  2 porty 1Gbit przeznaczone do zarządzania macierzą  Min. 8 portów 25Gb iSCSI  Min. 8 portów FC 32 Gb/s |
| **Poziomy RAID** | Macierz musi umożliwiać budowę jednego obszaru danych na wszystkich dyskach wewnątrz macierzy. Dyski muszą być skonfigurowane w taki sposób, aby utrata jednego z nich zapewniła ciągłość dostępu do danych.  Macierz musi posiadać skonfigurowaną wydzieloną przestrzeń spare-space zgodnie z zaleceniami producenta. |
| **Integracja z aplikacjami** | Oferowana macierz dyskowa musi zostać dostarczona z oprogramowaniem umożliwiającym zarządzanie i automatyzację procesów replikacji oraz ochrony danych z wykorzystaniem mechanizmu migawek (snapshots). Konieczne jest zapewnienie efektywnego tworzenia i przywracania kopii zapasowych, a także szybkiego odzyskiwania danych z uwzględnieniem ich spójności z wykorzystaniem migawek. Oferowane rozwiązanie powinno oferować integrację z istniejącymi aplikacjami zamawiającego (MS Exchange) oraz bazami danych (Oracle RAC, MS SQL), zapewniając możliwość optymalizacji i synchronizacji procesów ochrony danych (migawki i replikacja). Wymagane jest, aby oprogramowanie to wspierało zarówno środowiska wirtualne, jak i fizyczne.  Zamawiający wymaga aby dostarczona funkcjonalność była realizowana przez dedykowane oprogramowanie producenta macierzy. |
| **Bezpieczeństwo** | Wymaganie jest aby oferowana macierz dyskowa umożliwiała wdrożenie uwierzytelniania wieloskładnikowego (MFA) poprzez integrację z RSA SecurID. Uwierzytelnianie wieloskładnikowe musi zapewniać dodatkową warstwę zabezpieczeń podczas procesów logowania lub wykonywania transakcji w obrębie macierzy dyskowej.  Funkcjonalność ta musi być realizowane przez kontrolery macierzy. |
| **Funkcjonalności** | System musi obsługiwać natywną integrację z środowiskiem wirtualizacyjnym VMware za pomocą interfejsu VAAI (VMware vStorage API for Array Integration), umożliwiając przypisanie do podsystemu pamięci masowej operacji VMware, takich jak klonowanie/snap, replikacja vVol, monitoring wydajności i mechanizmu vMotion.  Rozwiązanie musi integrować się z wirtualnymi środowiskami poprzez dostarczenie przez producenta macierzy narzędzia do zarządzania i monitorowania.  Rozwiązanie musi obsługiwać funkcję Local Protection (Snapshot z technologią Redirect-On-Write dla danych blokowych i plikowych i Thin Clones), rozwiązania, które nie obsługują funkcji redirect on write nie są dozwolone.  Rozwiązanie musi obsługiwać replikację asynchroniczną na poziomie wirtualnych wolumenów (vVOL). Prezentacja replikowanych wirtualnych wolumenów musi się odbywać za pomocą protokołów SCSI oraz NVMe (rozdzielnie)  Należy dostarczyć oprogramowanie do wykonywania spójnych kopii danych aplikacji w minimum wersjach:  a)            Exchange 2016 i 2019, SQL Server 2017 i 2019, Oracle 18 i 19, VMware dla blokowych i plikowych datastore.  b)           Spójność kopii rozumieć należy jako funkcjonalność automatycznego przełączenia aplikacji w tryb wykonania spójnej kopii swoich danych.  c)            Oprogramowanie to musi rozpoznać, na których wolumenach logicznych aplikacja składuje swoje dane i wykonać kopie tylko tych wolumenów.  Macierz zarówno na poziomie jednej macierzy, jak i klastra – musi być zarządzana z poziomu jednej aplikacji, dostarczonej przez producenta urządzenia. Nie dopuszcza się dzielenia zarządzania pomiędzy różne aplikacje.  Urządzenie powinno na poziomie plikowym umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.  Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):   1. Możliwość zdjęcia blokady przed upływem ważności danych 2. Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE), w tym wypadku wymagane wsparcie norm SEC 17a-4(f) lub ISO Standard 15489-1 lub norm równoważnych w zakresie ochrony danych.   Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem na całą dostarczoną pojemność. |
| **Replikacja** | Ofertowana macierz musi wspierać replikację synchroniczną i asynchroniczną na poziomie zasobów blokowych oraz plikowych.  Replikowane pary wolumenów blokowych muszą mieć możliwość prezentacji do wybranego hosta lub grupy hostów za pomocą protokołu SCSI oraz NVMe (rozdzielnie).  Musi istnieć możliwość zmiany sposobu replikacji dla zasobów blokowych z synchronicznego na asynchroniczny i odwrotnie bez konieczności potrzeby zatrzymywania procesu replikacji.  Rozwiązanie musi obsługiwać dwukierunkową asynchroniczną zdalną replikację przez IP z opcją ustawienia relacji do: "1:1", "1:n", i "n:1". |
| **Quality of Service** | Oferowana macierz musi umożliwiać definiowanie polityk Quality of Service na podstawie następujących algorytmów z możliwością przypisania do hosta lub grupy hostów.:   1. Względne polityki wydajnościowe - definicja minimum trzech poziomów profili wydajnościowych 2. Bezwzględne polityki wydajnościowe - definicja na podstawie ilości IOPS oraz MB/s. 3. Bezwzględne polityki wydajnościowe - definicja na podstawie ilości IOPS oraz MB/s w przeliczeniu na wskazaną ilość danych w GB. 4. Bezwzględne polityki wydajnościowe - definicja na podstawie ilości IOPS oraz MB/s z możliwością warunkowego przekroczenia limitu o zadaną wielkość wyrażoną w procentach ustawionego limitu. |
| **Gwarancja** | Minimum 36 miesięcy gwarancji wsparcia producenta w miejscu instalacji. Możliwość zgłaszania awarii przez 24 godziny na dobę. Gwarantowany czas reakcji – następny dzień roboczy.  Zamawiający wymaga aby w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostał u Zamawiającego.  Macierz musi umożliwiać pracę oraz wdrożenie w środowisku całkowicie odizolowanym od dostępu do Internetu. |

### Przełącznik sieciowy SAN 2 szt.

|  |
| --- |
| **Wymagania minimalne** |
| Przełącznik FC musi być wykonany w technologii FC 64 Gb/s i posiadać możliwość pracy portów FC z prędkościami 64, 32 Gb/s z funkcją autonegocjacji prędkości. |
| Przełącznik FC musi posiadać minimum 24 sloty na moduły. Wszystkie wymagane funkcje muszą być dostępne dla minimum 16 portów FC przełącznika. |
| Przełącznik musi być dostarczony wraz z minimum 14 modułami SFP FC 32 Gb/s i 2 modułami SFP FC 32Gb/s LWL |
| Rodzaj obsługiwanych portów: F,E,Ex,D. |
| Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. |
| Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów. |
| Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów |
| Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN. |
| Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa:   * Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric * Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP * Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP * Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów * Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2, * Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric. * Konta użytkowników definiowane w środowisku RADIUS lub LDAP * Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS * Obsługa SNMP v3 |
| Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym. |
| Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC, USB port. |
| Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1) |
| Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP |
| Maksymalny dopuszczalny pobór mocy przełącznika FC to 105W |
| Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych. |
| Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN |
| Możliwość wymiany w trybie „na gorąco”: minimum w odniesieniu do modułów portów Fibre Channel (SFP+). |
| Wsparcie dla N\_Port ID Virtualization (NPIV). |
| Zamawiający wymaga min. 36 miesięcy gwarancji producenta z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. |
| Produkt musi być fabrycznie nowy i dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju. |
| Szyny do montażu w szafie rack. |

### Wkładki FC32Gb short wave 28 szt.

|  |
| --- |
| Wkładki kompatybilne z posiadanymi przełącznikami FC IBM |

### Wkładki FC32Gb long wave 4 szt.

|  |
| --- |
| Wkładki kompatybilne z posiadanymi przełącznikami FC IBM |

## LAN – urządzenia sieciowe

### Przełącznik sieciowy v1 4 szt.

|  |
| --- |
| Wymagane parametry minimalne:   * Minimum 16 portów 10/100/1000BASE-T wspierających standard 802.3at (PoE+) * Minimum 2 porty 1Gb SFP, pozwalające na instalację wkładek gigabitowych SFP. * Przepustowość: minimum 36 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika) * Wydajność: minimum 26 Mp/s * Tablica adresów MAC o wielkości minimum 16000 pozycji * Bufor pakietów nie mniejszy niż 1.5MB * Pamięć stała (typu Flash): minimum 512MB * Pamięć operacyjna: minimum 1GB * Budżet mocy dla PoE minimum 240W * Obsługa ramek Jumbo * Routing IPv4 * Routing IPv6 * Policy Based Routing * Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping * Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol * Obsługa sieci IEEE 802.1Q VLAN – minimum 4093 sieci VLAN * Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree * BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom * Wsparcie dla funkcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6) * Obsługa list ACL * Obsługa standardu 802.1p * Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP * Funkcja mirroringu portów lokalnego i zdalnego * Obsługa funkcji logowania do sieci („Network Login”) zgodna ze standardem IEEE 802.1x * LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED * Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC * TACACS+ i RADIUS Network Login * RADIUS Accounting * Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS * Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https * Syslog * Obsługa sFlow * Obsługa SNTP * Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania). * Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji). * Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian. * Wsparcie dla Private VLAN * Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych * Minimalny zakres pracy od -5°C do 50°C   Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. |

### Przełącznik sieciowy v2 11 szt.

|  |
| --- |
| Wymagane parametry minimalne:   * Minimum 48 portów 10/100/1000BASE-T * Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). * Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika) * Wydajność: minimum 130 Mp/s * Tablica adresów MAC o wielkości minimum 16000 pozycji * Bufor pakietów nie mniejszy niż 1.5MB * Pamięć stała (typu Flash): minimum 512MB * Pamięć operacyjna: minimum 1GB * Obsługa ramek Jumbo * Funkcja łączenia urządzeń w stosy z wykorzystaniem portów 10Gb/s i agregowanych portów 10Gb/s. Urządzenia połączone w stos widziane jako jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 200 portów. * Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain)) * Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie * Routing IPv4 * Routing IPv6 * Policy Based Routing * Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping * Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol * Obsługa sieci IEEE 802.1Q VLAN – minimum 4093 sieci VLAN * Obsługa IEEE 802.1ad QinQ i Selective QinQ * Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree * BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom * Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6) * Obsługa list ACL * Obsługa standardu 802.1p * Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); * Funkcja mirroringu portów lokalnego i zdalnego * Obsługa funkcji logowania do sieci („Network Login”) zgodna ze standardem IEEE 802.1x * LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED * Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC * TACACS+ i RADIUS Network Login * RADIUS Accounting * Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS * Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https * Syslog * Obsługa sFlow * Obsługa SNTP * Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania). * Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji). * Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian. * Wsparcie dla Private VLAN * Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych * Minimalny zakres pracy od -5°C do 50°C * Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. |

### Przełącznik sieciowy v3 11 szt.

|  |
| --- |
| Wymagane parametry minimalne:   * Minimum 48 portów 10/100/1000BASE-T wspierających standard 802.3at (PoE+) * Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). * Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika) * Wydajność: minimum 130 Mp/s * Tablica adresów MAC o wielkości minimum 16000 pozycji * Bufor pakietów nie mniejszy niż 1.5MB * Pamięć stała (typu Flash): minimum 512MB * Pamięć operacyjna: minimum 1GB * Budżet mocy dla PoE minimum 740W * Obsługa ramek Jumbo * Funkcja łączenia urządzeń w stosy z wykorzystaniem portów 10Gb/s i agregowanych portów 10Gb/s. Urządzenia połączone w stos widziane jako jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 200 portów. * Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain)) * Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie * Routing IPv4 * Routing IPv6 * Policy Based Routing * Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping * Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol * Obsługa sieci IEEE 802.1Q VLAN – minimum 4093 sieci VLAN * Obsługa IEEE 802.1ad QinQ i Selective QinQ * Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree * BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom * Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6) * Obsługa list ACL * Obsługa standardu 802.1p * Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); * Funkcja mirroringu portów lokalnego i zdalnego * Obsługa funkcji logowania do sieci („Network Login”) zgodna ze standardem IEEE 802.1x * LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED * Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC * TACACS+ i RADIUS Network Login * RADIUS Accounting * Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS * Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https * Syslog * Obsługa sFlow * Obsługa SNTP * Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania). * Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji). * Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian. * Wsparcie dla Private VLAN * Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych * Minimalny zakres pracy od -5°C do 50°C * Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji. |

### Przełącznik sieciowy v4 4 szt.

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| **Porty** | Przełącznik 1RU wyposażony w minimum 24 portów 25 Gigabit Ethernet SFP28, - minimum 4 porty  100GE QSFP28 oraz dodatkowo  -  port konsolowy RJ45   -  port  zarządzający typu out-of-band management    -  port  typu  USB |
| **System Operacyjny** | Musi być zgodny ze standardem ONIE i  umożliwiać instalacje systemów operacyjnych innych producentów, w celu uzyskania dodatkowych funkcjonalności. |
| **Pamięć** | Pamięć RAM co najmniej 8GB, pamięć bufora pakietów 32MB  i dysk SSD co najmniej 32GB |
| **Zasilanie** | 2 redundantne  zasilacze AC , możliwość wymiany w trakcie pracy urządzenia, możliwość instalacji zasilaczy DC |
| **Rack** | Musi zapewniać instalację w szafach 19” |
| **Wydajność** | Musi posiadać matrycę przełączającą o wydajności min. 2 Tbps (full-duplex), min. 1.4Bpps (full-duplex) |
| **Chłodzenie** | Musi posiadać możliwość chłodzenia urządzenia w trybie przód-do-tyłu lub tył-do-przodu (ustawienia fabryczne).  Musi być wyposażone w redundantne i wymienne w trakcie pracy (hot-swappable) wiatraki  Temperatura pracy w przedziale 0-45 stopni Celsjusza |
| **Obsługa warstwy II** | Obsługa protokołu PVST/ RPVST+ minimum 150 instancji  Obsługa mechanizmu Agregacji linków z protokołem LACP i statycznej oraz LACP fallback.  Co najmniej 128 logicznych interfejsów Port Channel, 32 porty per Port Channel  Obsługa protokołu UDLD lub podobnego  Obsługa protokołu IGMP snooping oraz DHCP snooping  Obsługa mechanizmu QinQ i Vlan translation  Obsługa min. 200 tysięcy adresów MAC |
| **Obsługa warstwy III** | Obsługa protokołu OSPFv2, co najmniej 120 interfejsów z włączonym OSPF  Obsługa protokołu BGP v4/v6, co najmniej 256 sąsiadów BGP  Obsługa protokołu BFD, co najmniej 64 sesje  Obsługa VRRP  Obsługa DHCP relay  Obsługa VRF, minimum 1000 VRF per przełącznik  Obsługa funkcjonalności NAT  Minimum 1000 interfejsów L3 per przełącznik  Obsługa minimum 128 tysięcy  wpisów routingu L3  Obsługa Layer 3 IGMP oraz PIM SSM dla multicast  Obsługa funkcjonalności IP SLA (ICMP/TCP track)  Waparcie dla Policy-Based Routing  Wsparcie dla EVPN  , L2VxLAN i L3VxLAN, co najmniej 512 tuneli VxLAN  Obsługa Symmetric IRB i Assymetric IRB oraz mechanizmu Arp Suppression  Wsparcie dla mechanizmu EVPN Multihoming |
| **Mechanizmy bezpieczeństwa** | Obsługa L2 ACL, L3 ACL, Receive ACL oraz Route map  Obsługa TACACS+, RADIUS i mechanizmu RBAC |
| **Funkcjonalności QoS** | Wsparcie dla L2 QoS i L3 Qos  Obsługa kolejkowania rcuchu (strict i WFQ) oraz WRED  Wsparcie dla ECN, Priority flow Control oraz BUM/Storm control |
| **Zarządzanie i monitoring** | Obsługa SSH, SCP,TFTP,NTP, SNMP v2/v3  Obsługa Zero Touch Deployment  Obsługa protokołu sflow  Obsługa SPAN i ESPAN |
| **Gwarancja** | Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. |

## Zestawy komputerowe

### Komputer typu All-in-One 176 szt.

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane parametry techniczne komputerów** | |
| **Typ** | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. | |
| **Zastosowanie** | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. | |
| **Obudowa** | Typu All-in-One zintegrowana z monitorem min. 23.8”. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej, demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi. Systemu montażowy VESA 100. Suma wymiarów obudowy bez zainstalowanego standu maks. 96cm. | |
| **Typowe parametry wyświetlacza** | Rozmiar i typ matrycy | 23,8” IPS lub WVA |
| Rozdzielczość | FHD (1920x1080) |
| Częstotliwość odświeżania | 60 Hz |
| Jasność | 250 cd/m² |
| Kontrast | 1500:1 |
| Barwa koloru | 99% sRGB |
| Poziome kąty widzenia | 178 stopni |
| Rodzaj matrycy | Matowa IPS |
| **Płyta główna** | Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min. 2 złącza SO - DIMM z obsługą do 64GB DDR5 pamięci RAM, min. 1 złącze M.2 dla dysku oraz 1 złącze M.2 karty WiFi. | |
| **Procesor** | Procesor musi być wyposażony w jednostki przetwarzania neuronowego (NPU) o wydajności co namniej 13 TOPS.  Procesor osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 31700 pkt. według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> zgodnie z wydrukiem stanowiącym załącznik do Zapytania Ofertowego (stan na 1.12.2025). | |
| **Pamięć RAM** | 16GB DDR5 5600 MT/s. Jeden slot pozostaje wolny. | |
| **Pamięć masowa** | Dysk M.2 SSD 512GB PCIe NVMe | |
| **Wydajność grafiki** | Zintegrowana karta graficzna. | |
| **Komunikacja** | Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika). | |
| **Wyposażenie multimedialne** | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki o mocy 2W każdy.  Wbudowana w obudowę matrycy cyfrowa kamera Full HD mechanicznie chowana w obudowie (nie dopuszcza się kamer przekręcanych i wystających poza obrys obudowy).  Wbudowane w obudowę dwa mikrofony.  Wbudowany w obudowę czytnik kart pamięci SD 4.0 (nie dopuszcza się stosowania zewnętrznych czytników USB). | |
| **Porty** | Porty wlutowane w płytę główną i wyprowadzone bezpośrednio bez stosowania przejściówek, adapterów, rozgałęziaczy itp.:  1 x USB 3.2 Gen 2 Typu A  2 x USB 3.2 Gen 1 Typu A  1 x USB 3.2 Gen 2 Typu C  2 x USB 2.0  1 x Port Audio combo (słuchawki i mikrofon)  1 x DisplayPort 1.4 (wyjście wideo) | |
| **Bezpieczeństwo** | Dedykowany układ sprzętowy TPM min. 2.0.  Komputer musi być wyposażony w czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym.  Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (wbudowane w obudowę gniazdo blokady Kensington) oraz kłódki (oczko w obudowie do założenia kłódki). | |
| **BIOS/UEFI** | Możliwość odczytania z BIOS informacji o:   * Wersji BIOS * Numerze seryjnym komputera * Numerze inwentarzowym * Typie (modelu) procesora, ilości rdzeni. * Zaimplementowanej sprzętowej technologii zdalnego zarządzania (o ile występuje). * Ilości pamięci RAM, jej prędkości oraz obsadzeniu w slotach. * Pojemności i modelu zainstalowanego dysku. * MAC adresie zintegrowanej karty sieciowej   BIOS musi umożliwiać:   * Włączenie/wyłączenie zintegrowanej karty sieciowej * Włączenie/wyłączenie karty sieci bezprzewodowej oraz Bluetooth (o ile występuje) * Włączenie/wyłączenie karty audio * Włączenie/wyłączenie poszczególnych portów USB   Powyższa funkcjonalność musi być realizowana wyłącznie poprzez BIOS. Nie dopuszcza się realizacji poprzez dodatkowe oprogramowanie, takie jak np. System diagnostyczny. | |
| **BIOS/UEFI bezpieczeństwo** | W celu zapewnienia możliwie najwyższego poziomu bezpieczeństwa danych organizacji, BIOS/UEFI musi umożliwiać:   * Nadanie hasła administratora * Ustawienie hasła dla zainstalowanego dysku * Ustawienie portów USB w trybie „No BOOT” * Zarządzanie funkcją Wake on Lan oraz PXE Boot zintegrowanej karty sieciowej * Zarządzanie funkcją Secure Boot * Zarządzanie układem TPM * Zarządzania funkcją tworzenia recovery BIOS * Zarządzania funkcją downgrade BIOS. * Zarządzanie czujnikiem otwarcia obudowy * Zapisywanie incydentów w formacie tzw. logów z możliwością ich przejrzenia. * Bezpieczne usuwanie danych z zainstalowanego dysku zgodnie z wytycznymi NIST 800-88r1 * Nadanie numeru inwentarzowego bezpośrednio w BIOS bez użycia dodatkowego oprogramowania. Nadany numer nie może być edytowalny w BIOS ani nie może ulec skasowaniu po jego aktualizacji. * Możliwość nadania hasła uniemożliwiającego rozruch systemu operacyjnego, możliwość zmiany tego hasła w BIOS musi być zachowana także po nadaniu hasła administratora. * Możliwość blokowania upgrade BIOS przez system operacyjny. * Blokowanie downgrade BIOS w celu zapewnienia kompatybilności z poprawkami systemu operacyjnego.   Powyższa funkcjonalność musi być realizowana wyłącznie poprzez BIOS. Nie dopuszcza się realizacji poprzez dodatkowe oprogramowanie, takie jak np. System diagnostyczny. | |
| **Oprogramowanie diagnostyczne** | System diagnostyczny z graficznym interfejsem użytkownika, działający poza środowiskiem systemu operacyjnego, dostępny z poziomu BIOS lub szybkiego menu boot’owania.  System umożliwiający przetestowanie komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności. Pełna obsługa systemu diagnostycznego za pomocą klawiatury i myszy jak i samej myszy. | |
| **Zintegrowany wizualny system diagnostyczny** | Wbudowany wizualny system diagnostyczny, zlokalizowany w obudowie lub w przycisku włączania, działający w oparciu sygnalizację LED, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami poprzez zmianę statusów wyświetlania diody (miganie w określonej sekwencji oraz zmiana barw wyświetlania).  System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS’u, awarię procesora.  Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. | |
| **Zasilacz** | Zewnętrzny zasilacz o mocy maks. 180W i efektywności średniej na poziomie min. 87% bez względu na poziom obciążenia. | |
| **Wirtualizacja** | Sprzętowe wsparcie technologi wirtualizacji realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). | |
| **System operacyjny** | Zainstalowany system operacyjny Windows 11 Pro, klucz licencyjny musi być zapisany trwale w BIOS i umożliwiać reinstalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. | |
| **Certyfikaty i standardy** | Certyfikat ISO 9001 lub równoważny dla producenta komputera  Certyfikat ISO 14001 lub równoważny dla producenta komputera  Certyfikat ISO 50001 lub równoważny dla producenta komputera  Deklaracja zgodności CE (załączyć do oferty)  Certyfikat EPEAT Silver dla oferowanego modelu komputera, dla Polski lub kraju członkowskiego UE – do oferty należy załączyć wydruk ze strony https://www.epeat.net/search-computers-and-displays - załączyć do oferty wydruk z strony  Certyfikaty ISO oraz deklaracja zgodności muszą być wystawione dla tego samego producenta sprzętu. Za producenta uznaje się każda osobę fizyczną lub prawną albo jednostkę organizacyjną nie posiadającą osobowości prawnej dla której ten wyrób zaprojektowano lub wytworzono, w celu wprowadzenia go do obrotu lub oddania do użytku pod własną nazwą lub znakiem. Certyfikaty ISO winny być możliwe do obejrzenia/pobrania z oficjalnych stron www producenta sprzętu.  Urządzenie musi spełniać kryteria środowiskowe, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gramów. | |
| **Ergonomia** | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 lub równoważną oraz wykazana zgodnie z normą ISO 9296 lub równoważną w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 28dB. | |
| **Wymagania dodatkowe** | * Klawiatura przewodowa USB w układzie polski programisty, sygnowana przez producenta jednostki centralnej. * Mysz optyczna przewodowa USB z dwoma przyciskami oraz rolką (scroll) sygnowana przez producenta jednostki centralnej. * Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu. * Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz musi być wpisany na stałe w BIOS. * Wraz z komputerem należy dostarczyć dedykowany przez producenta komputera podstawę, montowaną do jednostki w sposób niewymagający użycia jakichkolwiek narzędzi. * Podstawa jednostki typu All – in – One musi umożliwiać: * Regulację pochyłu pionowego w zakresie od -5 do 30 stopni. * Regulację wysokości w zakresie minimum 10 cm. * Ustawienie jednostki w trybie Pivot. * Obrót podstawy w lewą oraz prawą stronę. | |
| **Wsparcie techniczne producenta** | Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie). | |
| **Warunki gwarancji** | Firma serwisująca musi posiadać ISO 9001 lub równoważny na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.  Minimalny czas trwania wsparcia technicznego producenta wynosi 3 lata, z możliwością odpłatnego  przedłużenia tego okresu do 4 lub 5 lat od daty dostawy.  Sposób realizacji usług wsparcia technicznego:   * Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17. * Dedykowany bezpłatny portal online producenta do zgłaszania usterek i zarządzania zgłoszeniami serwisowymi. * Opcjonalna pomoc techniczna za pośrednictwem czat online.   Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii.  W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzien roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego.  Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta.  Mozliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń z nieaktywnym wsparciem technicznym.  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Zamawiający wymaga narzędzia do zarządzania zgłoszeniami serwisowymi samodzielnie przez portal internetowy lub inne narzędzie nie wymagające działań po stronie dostawcy. Narzędzie powinno umożliwiać:   * samodzielne wystawianie zgłoszeń serwisowych, śledzenie stanu zgłoszenia, komunikację z serwisem producenta przez edycję zlecenia i stanu zlecenia * dostęp do materiałów serwisowych - co najmniej podręczników serwisowych i not serwisowych * dostęp do materiałów szkoleniowych * możliwości dodawania plików do otwieranego lub otwartego zlecenia (zdjęcia uszkodzeń, opisy etc.) * śledzenie historii zleceń - raporty ze zleceń, historia - dla poszczególnych zleceń lub dla poszczególnych komputerów * możliwość samodzielnego zarządzania wysyłką części (decyzja o zamówieniu części zamiennych i diagnostyka po stronie zamawiającego) * możliwość rejestrowania i zarządzania zdarzeniami serwisowymi - agregowania zdarzeń z oprogramowania zarządzającego dostarczonego przez producenta, możliwość konwertowania zdarzeń na zgłoszenia serwisowe do producenta - z poziomu narzędzia. * możliwość spięcia systemu serwisowego producenta z systemem helpdesk zamawiającego (dostępność API co najmniej dla opcji wystawienie zlecenia, sprawdzenie stanu zlecenia, raport zleceń) * tworzenia kont dla inżynierów serwisu z możliwością sprawdzenia statystyk wydajności / jakości ich pracy. | |
| **Dodatkowe oprogramanie** | Wykonawca dostarczy wraz z komputerem oprogramowanie producenta komputera które umożliwia pełne zarządzanie, monitoring, konfigurację a w szczególności: dystrybucję ustawień BIOS (zawierającego wcześniej zdefiniowane ustawienia jednakowe dla wszystkich), jednocześnie na wszystkich komputerach zgodnie z polityką bezpieczeństwa Zamawiającego. Oprogramowanie musi w pełni integrować się z Microsoft SCCM  Wykonawca dostarczy sterowniki w formacie dedykowanym dla Microsoft SCCM w celu dystrybucji za pomocą dołączonego oprogramowania producenta komputera zgodnie z polityką bezpieczeństwa Zamawiającego.  Zamawiający oczekuje oprogramowania zarządzającego produkowanego przez producenta i instalowanego przez producenta na etapie produkcji komputera. Program ma umożliwiać przynajmniej:   * monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów * powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu * powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów * śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem.   Dołączone do oferowanego komputera oprogramowanie z nieograniczoną licencją czasowo na użytkowanie umożliwiające:   * upgrade i instalacje wszystkich sterowników, dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, * możliwość przed instalacją sprawdzenia każdego sterownika, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji:                   a. o poprawkach i usprawnieniach dotyczących aktualizacji                  b. dacie wydania ostatniej aktualizacji                  c. priorytecie aktualizacji                  d. zgodność z systemami operacyjnymi                  e. jakiego komponentu sprzętu dotyczy aktualizacja | |

### Komputer stacjonarny 13 szt.

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane parametry techniczne komputerów** |
| **Typ** | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. |
| **Zastosowanie** | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. |
| **Obudowa** | Małogabarytowa typu Terminal, umożliwiająca montaż wewnątrz obudowy min. 2 szt. dysków M.2 SSD. Suma wymiarów obudowy mierzona po krawędziach obudowy nie może przekraczać 400 mm, waga komputera nie większa niż 1.45kg (bez zasilacza). |
| **Płyta główna** | Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logo producenta oferowanej jednostki dedykowana dla danego urządzenia wyposażona w sloty i złącza:   * 2 złącza SODIMM z obsługą do 64GB pamięci RAM DDR5, * 2 złącza M.2 dedykowane dla dysku SSD, * 1 złącze M.2 WLAN, |
| **Procesor** | Procesor musi być wyposażony w jednostki przetwarzania neuronowego (NPU) o wydajności co namniej 13 TOPS.  Procesor osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 31700 pkt. według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> wg wydruku stanowiącego załącznik do Zapytania ofertowego (stan na 1.12.2025) |
| **Pamięć RAM** | 16GB DDR5. Możliwość rozbudowy do min 64GB, min. dwa sloty pamięci. |
| **Pamięć masowa** | Dysk M.2 SSD 512GB PCIe NVMe. |
| **Wydajność grafiki** | Zintegrowana karta graficzna. |
| **Komunikacja** | Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika). |
| **Wyposażenie multimedialne** | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera o mocy 2W. Port słuchawek i mikrofonu (combo) |
| **Porty** | Porty wlutowane w płytę główną i wyprowadzone bezpośrednio bez stosowania przejściówek, adapterów, rozgałęziaczy itp.:  Panel przedni:   * 1 x Universal audio jack (słuchawki i mikrofon) * 1 x USB 3.2 Gen 1 typu A [5 Gbps] * 1 x USB 3.2 Gen 1 typu C [10 Gbps] * Panel tylny: * 1 x DisplayPort 1.4a * 1 x HDMI 2.1 * 2 x USB 3.2 Gen 1 typ A [5 Gbps] * 2 x USB 2.0 * 1 x RJ45 10/100/1000 |
| **Bezpieczeństwo** | Dedykowany układ sprzętowy TPM min. 2.0.  Komputer musi być wyposażony w czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym.  Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (wbudowane w obudowę gniazdo blokady Kensington) oraz kłódki (oczko w obudowie do założenia kłódki). |
| **BIOS/UEFI** | Możliwość odczytania z BIOS informacji o:   * Wersji BIOS * Numerze seryjnym komputera * Numerze inwentarzowym * Typie (modelu) procesora, ilości rdzeni, * Ilości pamięci RAM, jej prędkości oraz obsadzeniu w slotach. * Pojemności i modelu zainstalowanego dysku. * MAC adresie zintegrowanej karty sieciowej * Technologii zdalnego zarządzania (o ile występuje)   BIOS musi umożliwiać:   * Włączenie/wyłączenie zintegrowanej karty sieciowej * Włączenie/wyłączenie karty sieci bezprzewodowej oraz Bluetooth (o ile występuje) * Włączenie/wyłączenie karty audio * Włączenie/wyłączenie poszczególnych portów USB   Powyższa funkcjonalność musi być realizowana wyłącznie poprzez BIOS. Nie dopuszcza się realizacji poprzez dodatkowe oprogramowanie, takie jak np. System diagnostyczny. |
| **BIOS/UEFI bezpieczeństwo** | W celu zapewnienia możliwie najwyższego poziomu bezpieczeństwa danych organizacji, BIOS/UEFI musi umożliwiać:   * Nadanie hasła administratora * Ustawienie hasła dla zainstalowanego dysku * Ustawienie portów USB wtrybie „No BOOT” * Zarządzanie funkcją Wake on Lan oraz PXE Boot zintegrowanej karty sieciowej * Zarządzanie funkcją Secure Boot * Zarządzanie układem TPM * Zarządzania funkcją tworzenia recovery BIOS * Zarządzania funkcją downgrade BIOS. * Zarządzanie czujnikiem otwarcia obudowy * Zapisywanie incydentów w formacie tzw. logów z możliwością ich przejrzenia * Bezpieczne usuwanie danych z zainstalowanego dysku zgodnie z wytycznymi NIST 800-88r1 * Nadanie numeru inwentarzowego bezpośrednio w BIOS bez użycia dodatkowego oprogramowania. Nadany numer nie może być edytowalny w BIOS ani nie może ulec skasowaniu po jego aktualizacji. * Możliwość nadania hasła uniemożliwiającego rozruch systemu operacyjnego, możliwość zmiany tego hasła w BIOS musi być zachowana także po nadaniu hasła administratora. * Możliwość blokowania upgrade BIOS przez system operacyjny. * Blokowanie downgrade BIOS w celu zapewnienia kompatybilności z poprawkami systemu operacyjnego.   Powyższa funkcjonalność musi być realizowana wyłącznie poprzez BIOS. Nie dopuszcza się realizacji poprzez dodatkowe oprogramowanie, takie jak np. System diagnostyczny. |
| **Oprogramowanie diagnostyczne** | System diagnostyczny z graficznym interfejsem użytkownika, działający poza środowiskiem systemu operacyjnego, dostępny z poziomu BIOS lub szybkiego menu boot’owania.  System umożliwiający przetestowanie komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności. Pełna obsługa systemu diagnostycznego za pomocą klawiatury i myszy jak i samej myszy. |
| **Zintegrowany wizualny system diagnostyczny** | Wbudowany wizualny system diagnostyczny usytuowany na przednim panelu obudowy, działający w oparciu sygnalizację LED wbudowaną np. w przycisk włącznika komputera.  System służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami poprzez zmianę statusów wyświetlania diody (miganie w określonej sekwencji oraz zmiana barw wyświetlania).  System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS’u, awarię procesora.  Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. |
| **Zasilacz** | Zewnętrzny zasilacz o mocy max. 90W i efektywności średniej na poziomie min. 88% bez względu na poziom obciążenia  W celu weryfikacji informacja dostępna na oficjalnej stronie producenta komputera lub w oficjalnym dokumencie na stronnie producenta komputera [wskazać adres strony lub dokumentu], lub dostarczyć test przeprowadzony przez niezależną akredytowaną jednostkę badawczą potwierdzającą spełnienie wymagania. |
| **Wirtualizacja** | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |
| **System operacyjny** | Zainstalowany system operacyjny Windows 11 Pro, klucz licencyjny musi być zapisany trwale w BIOS i umożliwiać reinstalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. |
| **Certyfikaty i standardy** | Certyfikat ISO 9001 lub równoważny dla producenta komputera  Certyfikat ISO 14001 lub równoważny dla producenta komputera  Certyfikat ISO 50001 lub równoważny dla producenta komputera  Deklaracja zgodności CE  Certyfikat EPEAT Gold dla oferowanego modelu komputera, dla Polski – wydruk ze strony <https://www.epeat.net/search-computers-and-displays> załączyć do oferty wydruk z strony.  Certyfikaty ISO oraz deklaracja zgodności muszą być wystawione dla tego samego producenta sprzętu. Za producenta uznaje się każda osobę fizyczną lub prawną albo jednostkę organizacyjną nie posiadającą osobowości prawnej dla której ten wyrób zaprojektowano lub wytworzono, w celu wprowadzenia go do obrotu lub oddania do użytku pod własną nazwą lub znakiem. Certyfikaty ISO winny być możliwe do obejrzenia/pobrania z oficjalnych stron www producenta sprzętu.  Urządzenie musi spełniać kryteria środowiskowe, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gramów. |
| **Ergonomia** | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 lub równoważną oraz wykazana zgodnie z normą ISO 9296 lub równoważną w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 22dB. |
| **Wymagania dodatkowe** | * Klawiatura przewodowa USB w układzie polski programisty sygnowana przez producenta jednostki centralnej * Mysz optyczna przewodowa USB z dwoma przyciskami oraz rolką (scroll) sygnowana przez producenta jednostki centralnej * Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu. * Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz musi być wpisany na stałe w BIOS. |
| **Wsparcie techniczne producenta** | Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie). |
| **Warunki gwarancji** | Firma serwisująca musi posiadać ISO 9001 lub równoważną na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.  Minimalny czas trwania wsparcia technicznego producenta wynosi 3 lata, z możliwością odpłatnego  przedłużenia tego okresu do 4 lub 5 lat od daty dostawy.  Sposób realizacji usług wsparcia technicznego:   * Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17. * Dedykowany bezpłatny portal online producenta do zgłaszania usterek i zarządzania zgłoszeniami serwisowymi. * Opcjonalna pomoc techniczna za pośrednictwem czat online.   Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii.  W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzień roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego.  Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta.  Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń z nieaktywnym wsparciem technicznym.  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Zamawiający wymaga narzędzia do zarządzania zgłoszeniami serwisowymi samodzielnie przez portal internetowy lub inne narzędzie nie wymagające działań po stronie dostawcy. Narzędzie powinno umożliwiać:   * samodzielne wystawianie zgłoszeń serwisowych, śledzenie stanu zgłoszenia, komunikację z serwisem producenta przez edycję zlecenia i stanu zlecenia * dostęp do materiałów serwisowych - co najmniej podręczników serwisowych i not serwisowych * dostęp do materiałów szkoleniowych * możliwości dodawania plików do otwieranego lub otwartego zlecenia (zdjęcia uszkodzeń, opisy etc.) * śledzenie historii zleceń - raporty ze zleceń, historia - dla poszczególnych zleceń lub dla poszczególnych komputerów * możliwość samodzielnego zarządzania wysyłką części (decyzja o zamówieniu części zamiennych i diagnostyka po stronie zamawiającego) * możliwość rejestrowania i zarządzania zdarzeniami serwisowymi - agregowania zdarzeń z oprogramowania zarządzającego dostarczonego przez producenta, możliwość konwertowania zdarzeń na zgłoszenia serwisowe do producenta - z poziomu narzędzia. * możliwość spięcia systemu serwisowego producenta z systemem helpdesk zamawiającego (dostępność API co najmniej dla opcji wystawienie zlecenia, sprawdzenie stanu zlecenia, raport zleceń) * tworzenia kont dla inżynierów serwisu z możliwością sprawdzenia statystyk wydajności / jakości ich pracy. |
| **Dodatkowe oprogramanie** | Wykonawca dostarczy wraz z komputerem oprogramowanie producenta komputera które umożliwia pełne zarządzanie, monitoring, konfigurację a w szczególności: dystrybucję ustawień BIOS (zawierającego wcześniej zdefiniowane ustawienia jednakowe dla wszystkich), jednocześnie na wszystkich komputerach zgodnie z polityką bezpieczeństwa Zamawiającego. Oprogramowanie musi w pełni integrować się z Microsoft SCCM  Wykonawca dostarczy sterowniki w formacie dedykowanym dla Microsoft SCCM w celu dystrybucji za pomocą dołączonego oprogramowania producenta komputera zgodnie z polityką bezpieczeństwa Zamawiającego.  Zamawiający oczekuje oprogramowania zarządzającego produkowanego przez producenta i instalowanego przez producenta na etapie produkcji komputera. Program ma umożliwiać przynajmniej:   * monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów * powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu * powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów * śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem.   Dołączone do oferowanego komputera oprogramowanie z nieograniczoną licencją czasowo na użytkowanie umożliwiające:   * upgrade i instalacje wszystkich sterowników, dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, * możliwość przed instalacją sprawdzenia każdego sterownika, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji:                   a. o poprawkach i usprawnieniach dotyczących aktualizacji                  b. dacie wydania ostatniej aktualizacji                  c. priorytecie aktualizacji                  d. zgodność z systemami operacyjnymi                  e. jakiego komponentu sprzętu dotyczy aktualizacja |

### Pakiet biurowy 189 szt.

|  |
| --- |
| Pakiet oprogramowania biurowego Microsoft Office Home & Business lub równoważny  Wymagania:   * Licencja wieczysta w najnowszej dostępnej wersji * Licencja dedykowana dla klienta biznesowego, zgodna z licencjonowaniem producenta * Polska wersja językowa   Zawierająca moduły:   * Arkusz kalkulacyjny * Edytor tekstów * Edytor prezentacji * Program poczty elektronicznej * Notatnik   **Warunki równoważności:**   * Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) * Tworzenie i edycja dokumentów elektronicznych w ustalonym formacie spełniającym warunki: * kompletny i publicznie dostępny opis formatu * zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika nr 2 do Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773) * umożliwia wykorzystanie schematów XML * Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców. * W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). * Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.   **Edytor tekstów musi umożliwiać:**   * Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. * Wstawianie oraz formatowanie tabel. * Wstawianie oraz formatowanie obiektów graficznych. * Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). * Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. * Automatyczne tworzenie spisów treści. * Formatowanie nagłówków i stopek stron. * Sprawdzanie pisowni w języku polskim. * Śledzenie zmian wprowadzonych przez użytkowników. * Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. * Określenie układu strony (pionowa/pozioma). * Wydruk dokumentów. * Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. * Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu * Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. * Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem. * Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa. * Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy zgodnie z wymaganiami obowiązującego w Polsce prawa.   **Arkusz kalkulacyjny musi umożliwiać:**   * Tworzenie raportów tabelarycznych. * Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych. * Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. * Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice). * Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych. * Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. * Wyszukiwanie i zamianę danych. * Wykonywanie analiz danych przy użyciu formatowania warunkowego. * Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. * Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. * Formatowanie czasu, daty i wartości finansowych z polskim formatem. * Zapis wielu arkuszy kalkulacyjnych w jednym pliku. * Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. * Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji   **Edytor prezentacji musi umożliwiać:**   * Przygotowywanie prezentacji multimedialnych. * Prezentowanie przy użyciu projektora multimedialnego. * Drukowanie w formacie umożliwiającym robienie notatek. * Zapisanie jako prezentacja tylko do odczytu. * Nagrywanie narracji i dołączanie jej do prezentacji. * Opatrywanie slajdów notatkami dla prezentera. * Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo. * Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego. * Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym. * Możliwość tworzenia animacji obiektów i całych slajdów. * Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. * Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007 i 2010.   **Program poczty elektronicznej musi umożliwiać:**   * Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego. * Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców. * Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną. * Automatyczne grupowanie poczty o tym samym tytule. * Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy. * Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia. * Zarządzanie kalendarzem. * Udostępnianie kalendarza innym użytkownikom. * Przeglądanie kalendarza innych użytkowników. * Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach. * Zarządzanie listą zadań. * Zlecanie zadań innym użytkownikom. * Zarządzanie listą kontaktów. * Udostępnianie listy kontaktów innym użytkownikom * Przeglądanie listy kontaktów innych użytkowników. * Możliwość przesyłania kontaktów innym użytkowników |

## Backup danych

### Urządzenie do przechowywania i deduplikacji danych 1 szt.

|  |  |
| --- | --- |
| **Lp.** | **Parametr wymagany** |
|  | Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli. |
|  | Dostarczone urządzenie musi oferować przestrzeń min. 20TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji – przestrzeń dedykowana do gromadzenia deduplikatów, wymagana skalowalność do min. 250TB netto (powierzchni użytkowej widocznej po założeniu systemu plików) |
|  | Dostarczone urządzenie musi umożliwiać rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityka retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę, wymagane wsparcie dla dla AWS, Microsoft Azure oraz Google GCP. Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń min. 80TB netto dla warstwy CLOUD. |
|  | Oferowane urządzenie musi posiadać minimum   * 4 porty 10/25Gb/s Eth OP   wymagana możliwość obsługi każdym z w/w portów protokołów CIFS, NFS, deduplikacja na źródle  wymagana możliwość dodania do w/w konfiguracji portów:   * 4 porty FC 32Gb/s   wymagana możliwość obsługi poprzez porty FC protokołów VTL oraz deduplikacja na źródle  ( możliwość dodania dwóch portów FC oznacza oficjalnie wsparcie takiej konfiguracji przez producenta urządzenia, wolny slot na dodatkowa kartę HBA w przypadku oferowanej konfiguracji urządzenia oraz możliwość natychmiastowego zamówienia u producenta wymaganej karty rozszerzeń) |
|  | Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami:   * CIFS, NFS * zapewniającym deduplikację na źródle, wymagane wsparcie dla aplikacji Commvault lub równoważnej (co najmniej na poziomie Media Server a także Client Direct przy użyciu storage accelerator), Veeam Backup and Replication lub równoważnej (co najmniej na poziomie Veeam Data Mover), NetWorker na poziomie standardowego klienta * VTL (min. 10 jednocześnie) |
|  | Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, deduplikacja na źródle, VTL do oferowanej pojemności urządzenia |
|  | Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: **NFS** co najmniej 25 TB/h (dane podawane przez producenta) oraz co najmniej 50 TB/h z wykorzystaniem **deduplikacji na źródle** (dane podawane przez producenta). |
|  | Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie:   * zapis danych minimum 150 strumieniami * odczyt danych minimum 50 strumieniami * replikacja minimum 50 strumieniami   pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.  Wymienione wartości 250 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu i jednocześnie 50 strumieni dla odczytu i jednocześnie 50 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.  Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji. |
|  | Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych:   * StorageTek L180 * IBM TS 3500 |
|  | Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7 |
|  | Urządzenie musi umożliwiać (w przypadku VTL’a) emulację minimum 250 napędów, emulację min. 30 000 slotów w przypadku poj. biblioteki taśmowej oraz emulację sumarycznie min. 60 000 slotów. |
|  | Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia. |
|  | Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o wielkości nie większej niż 12 kB.  Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości. |
|  | Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również muszą podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A”, nie może zostać ponownie zapisany jeśli trafi do innej wirtualnej biblioteki „B” w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych. |
|  | Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. Wymaganie nie będzie spełnione jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backup’ową. Wymaganie deduplikacji in-line dotyczy zapisu danych przez każdy z wymaganych intefejsów, w przypadku interfejsów: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie może w żadnym stopniu zależeć od konkretnej aplikacji backu’owej, dane zapisywane poprzez interfejsy NFS CIFS bez użycia jakiejkolwiek aplikacji backup’owej również muszą być deduplikowane w sposób in-line |
|  | Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line) |
|  | Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane. |
|  | Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymaganie dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych. |
|  | Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Commvault, Veeam Backup and Replication, NetWorker.  W przypadku współpracy z każdą z poniższych aplikacji:   * Commvault * Veeam Backup and Replication * NetWorker   urządzenie musi umożliwiać deduplikację na źródle (w przypadku Commvault: co najmniej na poziomie Media Server a także Client Direct przy użyciu storage accelerator, w przypadku Veeam Backup and Replication co najmniej na poziomie Veeam Data Mover), w przypadku NetWorker na poziomie standardowego klienta) i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby do oferowanego urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
|  | W przypadku przyjmowania backupów z Commvault, Veeam Backup and Replication, NetWorker, urządzenie musi umożliwiać deduplikację na źródle (co najmniej na poziomie Media Server dla CommVault, Data Mover dla Veeam, klienta dla NetWorker) i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby do oferowanego urządzenia były transmitowane poprzez sieć FC jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
|  | Oferowane urządzenie musi umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych. |
|  | Wymagana funkcjonalność Load Balancing oraz Link Failover w obrębie portów (Eth) wykorzystywanych przez aplikację backupową. |
|  | Wymagane wsparcie dla backupów typu Virtual Synthetics w przypadku aplikacji Commvault, Veeam Backup and Replication oraz NetWorker. |
|  | W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów. |
|  | Urządzenie musi umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia. |
|  | Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych:   * Windows * Linux (RedHat, SuSE) |
|  | Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów:   * jeden do jednego * wiele do jednego * jeden do wielu * kaskadowej (urządzenie A replikuje dane do urządzania B, które te same dane replikuje do urządzenia C).   Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację jest przedmiotem postępowania. |
|  | Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji. |
|  | W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. |
|  | W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana możliwość kontroli przez: Commvault oraz NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:   * replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących * replikacji podlegają tylko te fragmenty danych (na poziomie bloków używanych do deduplikacji), które nie znajdują się na docelowym urządzeniu * replikacja zarządzana jest z poziomu wymaganej aplikacji * aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji |
|  | Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%. |
|  | Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie musi być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji. |
|  | Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej. |
|  | Oferowane urządzenie musi pozwalać na realizację oraz przechowywanie SnapShot’ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot’u.  Odtworzenie danych ze Snapshot’u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów). |
|  | Urządzenie musi pozwalać na przechowywanie minimum 500 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności. |
|  | Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia). |
|  | Urządzenie musi mieć możliwość podziału na minimum 10 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 10 logicznych części pracujących równolegle z pełną wydajnością urządzenia. |
|  | Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. |
|  | Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia jako niezależnego urządzenia dostępnego za pośrednictwem:   * CIFS * NFS * VTL * deduplikacja na źródle |
|  | Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.  Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):   1. Możliwość zdjęcia blokady przed upływem ważności danych 2. Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE), w tym wypadku wymagane wsparcie norm SEC 17a-4(f) lub równoważnych oraz ISO Standard 15489-1 lub równoważnych w zakresie ochrony danych, wymagane oficjalne wsparcie wymaganej blokady przez aplikację Commvault, Veeam Backup and Replication oraz NetWorker – wymagane potwierdzenie na oficjalnych stronach w/w aplikacji backup’owych oraz producenta oferowanego deduplikatora   Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem.  Wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady. W każdym przypadku wymagana również możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności SnapShot. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności). |
|  | Urządzenie musi mieć możliwość przechowywania danych niezmienialnych:   * Video * Grafika * Nagrania dźwiękowe * Pliki pdf   na udziałach CIFS/NFS. |
|  | Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie, ale o weryfikację wszystkich zabezpieczanych danych backup’owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja musi być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność. Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności). |
|  | Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia. |
|  | Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu). |
|  | Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora), wymagane potwierdzenie w ogólnodostępnej dokumentacji. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności) |
|  | Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication. |
|  | Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas, w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta). |
|  | Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni realizowanego w sposób automatyczny lub innego dowolnie definiowanego progu powyżej 50% zajętości. |
|  | Urządzenie musi mieć możliwość zarządzania poprzez   * Interfejs graficzny dostępny z przeglądarki internetowej * Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell) |
|  | Oprogramowanie do zarządzania musi rezydować na oferowanym urządzeniu deduplikacyjnym. |
|  | Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade’ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem. |
|  | Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania. |
|  | Oferowane urządzenie musi być objęte min. 3 letnim wsparciem producenta działającym w trybie zgłaszania awarii: 24x7 oraz reakcją NBD. |

### Serwer backupu 1 szt.

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Obudowa Rack o wysokości max. 2U, umożliwiającą instalację min. 12 dysków 3,5” i 2 dysków 2,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.  Możliwość instalacji karty umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne  - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 334 punktów w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. Dla oferowanego serwera. |
| **RAM** | Min. 64GB DDR5 RDIMM 5600MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| **Zabezpieczenia pamięci RAM** | Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection (PFD) |
| **Sloty PCIe** | Min. jeden slot PCIe x16 , min. jeden slot PCIe x8 oraz jeden slot OCP 3.0. |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT  Dwa interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 nie zajmujące slotów PCIe.  Dodatkowo zainstalowane:  - jedna karta dwuportowa FC 32Gb/s |
| **Dyski twarde** | Zainstalowane 2 x 480GB SSD SATA oraz 12 x 8TB SATA 7.2k.  Zainstalowane dwa dyski hot-swap M.2 NVMe o pojemności min. 480GB z możliwością konfiguracji RAID 1. |
| **Kontroler RAID** | Zainstalowany kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. |
| **Wbudowane porty** | min. port USB 2.0 oraz dwa porty USB 3.0, port VGA |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900 |
| **Wentylatory** | Redundantne |
| **Zasilacze** | Min. dwa zasilacze Hot-Plug maksymalnie 700W Titanium. |
| **Bezpieczeństwo** | Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.  Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą  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.  Możliwość integracji z RSA SecurID |
| **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 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.   Karta powinna umożliwiać rozszerzenie funkcjonalności o:   * możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych * 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 |
| **Oprogramowanie do zarządzania** | Możliwość instalacji oprogramowania producenta do zarządzania, spełniające 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. |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 lub równoważnej oraz ISO-14001 lub równoważnej.  Serwer musi posiadać deklaracja CE.  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub równoważną.  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2019 x64, Microsoft Windows 2022 x64, Microsoft Windows 2025. |
| **Normy Środowiskowe** | 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 rozporządzenia nr 1272/2008WE. 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 potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019***.***  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. |
| **Warunki gwarancji** | Zamawiający wymaga min. 36 miesiące gwarancji producenta możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365  następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.  Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej  (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik ***producenta*** z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następny dzień roboczy od zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi sie na inną formę. |
| **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. |

### Oprogramowania backupu danych 1 szt.

|  |  |
| --- | --- |
| **Kategoria** | **Charakterystyka (wymagania minimalne)** |
| **Wymagania ogólne** | * Zamawiający wymaga dostarczenia licencji oprogramowania w formie 3-letniej subskrypcji. * Licencja musi umożliwiać backup 40 maszyn wirtualnych. * Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner Peer Insights: i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5, * Oprogramowanie musi współpracować z infrastrukturą VMware w wersji, 7.x i 8.0 oraz Microsoft Hyper-V 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej. * Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.5.x - 7.0, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4 lub nowszy oraz Proxmox VE 8.2 lub nowszy. * Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. |
| **Całkowite koszty posiadania** | * Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej * Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków * Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji * Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. * Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych to takiej puli. * Oprogramowanie musi pozwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta. * Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. * Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. * Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania * Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time) * Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu * Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API * Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji * Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji * Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania * Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. * Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej * Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np. skasowanie backupu, dodanie kolejnego administratora) * Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS) * Oprogramowanie musi posiadać integracje z systemami typu SIEM * Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji. |
| **Wymagania RPO** | * Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej * Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. * Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna co najmniej dla platformy VMware i Hyper-V * Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware. * Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. * Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592). * Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) * Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. * Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. * Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. * Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. * Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. * Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik * Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) * Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |
| **Wymagania RTO** | * Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. * Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) * Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami * Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere * Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. * Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków * Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. * Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików * Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. * Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell * Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM * Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. * Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. * Oprogramowanie musi pozwalać na backup i odtwarzanie usługi Entra ID. W szczególności użytkowników, grupy, role, jednostki administracyjne, entrprise applications oraz logi audytowe i sign-in. * Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. * Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. * Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. * Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. * Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. * Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. * Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji * Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN * Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle * Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI * Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2 * Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |
| **Ograniczenie ryzyka** | * Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) * Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych * Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem * Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. * Oprogramowanie musi posiadać swój wbudowany program antywirusowy zoptymalizowany do przeszukiwania kopii backupowych * Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware * Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania * Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków * Oprogramowanie musi posiadać mechanizm wykrywania oznak ataku hakerskiego tzw. Indicators of Compromise * Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. * Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR |
| **Środowiska fizyczne** | * Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego * Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych * Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, Rocky Linux, AlmaLinux * Rozwiązanie musi wspierać system operacyjny macOS * Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix * Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) * Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster * Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów * Rozwiązanie musi wspierać backup podłączonych dysków USB * Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym * Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) * Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone * Rozwiązanie musi wspierać kontrolę pasma sieciowego * Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych * Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN * Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft * Rozwiązanie musi wspierać technologię BitLocker * Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania * Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych * Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych * Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle i PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu. * Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform * Rozwiązanie musi wspierać szyfrowanie * Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne * Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego * Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej * Rozwiązanie musi wspierać tworzenie wielu zadań backupowych |
| **Monitoring** | * System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich * System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie * System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2016, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. * System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter * System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn * System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel * System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk * System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora * System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów * System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) * System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna * System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego * System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta * System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. * System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. * System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware |
| **Raportowanie** | * System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie * System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V, 2019, 2022 oraz 2025 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. * System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. * System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V * System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF * System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc * System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach * System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów * System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych * System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych * System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury * System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta * System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. * System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’. * System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware * System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) * System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie |

## Cyberbezpieczeństwo

### Urządzenie UTM v1 2 szt.

|  |  |
| --- | --- |
| **Kategoria** | **Charakterystyka (wymagania minimalne)** |
| **Wymagania ogólne** | * System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. * System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. * System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. * Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. * System wspiera protokoły IPv4 oraz IPv6 w zakresie:   + Firewall.   + Ochrony w warstwie aplikacji.   + Protokołów routingu dynamicznego. |
| **Redundancja, monitoring i wykrywanie awarii** | * W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. * Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. * Monitoring stanu realizowanych połączeń VPN. * System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |
| **Interfejsy, Dysk, Zasilanie** | * System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:   + 8 portami Gigabit Ethernet RJ-45.   + 4 gniazdami SFP 1 Gbps.   + 8 gniazdami SFP+ 10 Gbps. * System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. * System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. * System jest wyposażony w zasilanie 2xAC. |
| **Parametry wydajnościowe** | * W zakresie Firewall’a obsługa nie mniej niż 10 mln jednoczesnych połączeń oraz 380 tys. nowych połączeń na sekundę. * Przepustowość Stateful Firewall: nie mniej niż 38 Gbps dla pakietów 512 B. * Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 26 Gbps. * Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 35 Gbps. * Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 9 Gbps. * Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 6 Gbps. * Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 6 Gbps. |
| **Funkcje Systemu Bezpieczeństwa** | * W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   + Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.   + Kontrola Aplikacji.   + Poufność transmisji danych - połączenia szyfrowane IPSec VPN.   + Ochrona przed malware.   + Ochrona przed atakami - Intrusion Prevention System.   + Kontrola stron WWW.   + Kontrola zawartości poczty – Antyspam dla protokołów SMTP.   + Zarządzanie pasmem (QoS, Traffic shaping).   + Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.   + Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.   + Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.   + Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |
| **Polityki, Firewall** | * Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. * System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:   + Translację jeden do jeden oraz jeden do wielu.   + Dedykowany ALG (Application Level Gateway) dla protokołu SIP. * W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. * Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. * Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. * Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. * Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu:   + Amazon Web Services (AWS).   + Microsoft Azure.   + Cisco ACI.   + Google Cloud Platform (GCP).   + OpenStack.   + VMware NSX.   + Kubernetes. |
| **Połączenia VPN** | System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:   * Wsparcie dla IKE v1 oraz v2. * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19, 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.   Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |
| **Routing i obsługa łączy WAN** | W zakresie routingu rozwiązanie zapewnia obsługę:   * Routingu statycznego. * Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. * Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. * ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. * BFD (Bidirectional Forwarding Detection). * Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |
| **Funkcje SD-WAN** | * System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. * SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| **Zarządzanie pasmem** | * System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. * System daje możliwość określania pasma dla poszczególnych aplikacji. * System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. * System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |
| **Ochrona przed malware** | * Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). * Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. * W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. * System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. * System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). * Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. * System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. * Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. * Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| **Ochrona przed atakami** | * Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. * System chroni przed atakami na aplikacje pracujące na niestandardowych portach. * Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. * System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. * Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). * Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. * Wykrywanie i blokowanie komunikacji C&C do sieci botnet. * Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| **Kontrola aplikacji** | * Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. * Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. * Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. * Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. * Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). * System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |
| **Kontrola WWW** | * Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. * W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. * Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. * Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. * Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). * Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. * Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. * Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. * System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| **Uwierzytelnianie użytkowników w ramach sesji** | * System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:   + Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.   + Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.   + Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. * System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. * System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. * Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| **Zarządzanie** | * Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. * Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. * Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. * System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. * System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. * Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. * Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. * Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). * Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| **Logowanie** | * Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. * W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. * Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. * Możliwość włączenia logowania per reguła w polityce firewall. * System zapewnia możliwość logowania do serwera SYSLOG. * Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| **Testy wydajnościowe oraz funkcjonalne** | * Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni. |
| **Serwisy i licencje** | * Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: * Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy. |
| **Gwarancja oraz wsparcie** | * System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię. |

### Urządzenie UTM v2 2 szt.

|  |  |
| --- | --- |
| **Kategoria** | **Charakterystyka (wymagania minimalne)** |
| **Wymagania ogólne** | System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.  Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.  System wspiera protokoły IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. |
| **Redundancja, monitoring i wykrywanie awarii** | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.  Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.  Monitoring stanu realizowanych połączeń VPN.  System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |
| **Interfejsy, Dysk, Zasilanie** | System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:   * 8 portami Gigabit Ethernet RJ-45. * 8 gniazdami SFP+ 10 Gbps.   System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.  System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.  System jest wyposażony w zasilanie 2xAC. |
| **Parametry wydajnościowe** | W zakresie Firewall’a obsługa nie mniej niż 1.5 mln jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę.  Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B.  Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6 Gbps.  Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 25 Gbps.  Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 4 Gbps.  Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2 Gbps.  Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.5 Gbps. |
| **Funkcje Systemu Bezpieczeństwa** | W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   * Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. * Kontrola Aplikacji. * Poufność transmisji danych - połączenia szyfrowane IPSec VPN. * Ochrona przed malware. * Ochrona przed atakami - Intrusion Prevention System. * Kontrola stron WWW. * Kontrola zawartości poczty – Antyspam dla protokołów SMTP. * Zarządzanie pasmem (QoS, Traffic shaping). * Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. * Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. * Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. * Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |
| **Polityki, Firewall** | Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:   * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.   W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.  Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.  Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.  Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.  Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu:   * Amazon Web Services (AWS). * Microsoft Azure. * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. * Kubernetes. |
| **Połączenia VPN** | System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:   * Wsparcie dla IKE v1 oraz v2. * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19, 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.   Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |
| **Routing i obsługa łączy WAN** | W zakresie routingu rozwiązanie zapewnia obsługę:   * Routingu statycznego. * Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. * Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. * ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. * BFD (Bidirectional Forwarding Detection). * Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |
| **Funkcje SD-WAN** | System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.  SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| **Zarządzanie pasmem** | System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.  System daje możliwość określania pasma dla poszczególnych aplikacji.  System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.  System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |
| **Ochrona przed malware** | Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).  Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.  W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.  System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.  System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).  Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.  System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.  Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.  Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| **Ochrona przed atakami** | Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.  System chroni przed atakami na aplikacje pracujące na niestandardowych portach.  Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.  System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.  Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).  Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.  Wykrywanie i blokowanie komunikacji C&C do sieci botnet.  Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| **Kontrola aplikacji** | Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.  Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.  Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.  Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).  System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |
| **Kontrola WWW** | Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.  W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.  Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.  Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.  Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).  Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.  Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.  Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.  System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| **Uwierzytelnianie użytkowników w ramach sesji** | System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:   * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.   System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.  System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.  Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| **Zarządzanie** | Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.  Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.  Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.  System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.  System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.  Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.  Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.  Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).  Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| **Logowanie** | Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.  W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.  Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.  Możliwość włączenia logowania per reguła w polityce firewall.  System zapewnia możliwość logowania do serwera SYSLOG.  Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| **Testy wydajnościowe oraz funkcjonalne** | Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni. |
| **Serwisy i licencje** | Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:  Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, bazy reputacyjne adresów IP/domen na okres 36 miesięcy. |
| **Gwarancja oraz wsparcie** | System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię. |

### Oprogramowanie do zbierania oraz analizy logów sieciowych 1 szt.

|  |  |
| --- | --- |
| **Kategoria** | **Charakterystyka (wymagania minimalne)** |
| **Wymagania ogólne** | * W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. * Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi wersje 6.5 i nowsze; Microsoft Hyper-V wersje 2016 i nowsze; Citrix XenServer wersje 8.2 i nowsze, Open Source Xen 4.2.5, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP). |
| **Interfejsy, Dysk** | * System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB. |
| **Parametry wydajnościowe** | * System musi być w stanie przyjmować minimum 5 GB logów na dzień. * Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.   W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:  **- Logowanie**   * Podgląd logowanych zdarzeń w czasie rzeczywistym. * Możliwość przeglądania logów historycznych z funkcją filtrowania. * System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:   + Listę najczęściej wykrywanych ataków.   + Listę najbardziej aktywnych użytkowników.   + Listę najczęściej wykorzystywanych aplikacji.   + Listę najczęściej odwiedzanych stron www.   + Listę krajów , do których nawiązywane są połączenia.   + Listę najczęściej wykorzystywanych polityk Firewall.   + Informacje o realizowanych połączeniach IPSec. * Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. * Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. * System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.   **Raportowanie**  W zakresie raportowania system musi zapewniać:   * Generowanie raportów co najmniej w formatach: PDF, CSV. * Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. * Funkcję definiowania własnych raportów. * Możliwość spolszczenia raportów. * Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.   **Korelacja logów**  W zakresie korelacji zdarzeń system musi zapewniać:   * Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. * Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. * Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: * Malware. * Aplikacje sieciowe. * Email. * IPS. * Traffic. * Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.   **Zarządzanie**   * System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. * System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.   **Serwisy i licencje**   * System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. * System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. |

## Licencja na oprogramowanie antywirusowe

|  |
| --- |
| **Rozszerzenie funkcjonalności posiadanej licencji ESET PROTECT Essential na 230 stanowisk, ważnej do dnia 2026-03-23.**  **Wymagania:**  Posiadana licencja musi być rozszerzona do 300 stanowisk i obejmować 36 miesięcy od daty zakończenia aktualnie posiadanej licencji.  Licencja musi być rozszerzona o następujące moduły Eset:   * Sandbox w chmurze (LiveGuard Advanced) * Szyfrowanie dysków (Full Disk Encryption) * Endpoint Detection and Response / eXtended Detection and Response (Inspect)   Ochrona serwera pocztowego MS Exchange  Ochrona usług chmurowych Microsoft 365  Zarządzanie podatnościami Vulnerability Assessment and Patch Management  - Uwierzytelnianie wieloskładnikowe/MFA |

## Urządzenia sieci bezprzewodowej

### Punkt dostępowy WLAN 50 szt.

|  |
| --- |
| Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.   * Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:   + Temperatura 0–50°C,   + Wilgotność 5–90%. * Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington. * Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać co najmniej następujące standardy:   + 2.4 GHz 802.11b/g/n/ax,   + 5 GHz 802.11a/n/ac/ax,   + 6 GHz 802.11ax/be * Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID. * Urządzenie musi być wyposażone w moduł BLE. * Urządzenie musi być wyposażone w co najmniej jeden interfejs Ethernet (RJ45) wspierający co najmniej szybkości 1G/2.5G/5.0G. * Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz. Maksymalne zużycie energii nie może przekraczać 17W przy wykorzystaniu wszystkich funkcji urządzenia. * Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:   + Tunnel,   + Bridge,   + Mesh. * Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja. * Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST). * Interfejs radiowy urządzenia powinien wspierać następujące funkcje:   + MIMO – 2x2,   + Wymagana przepustowość dla poszczególnych modułów radiowych:   min. 688 Mbps;  min. 2882 Mbps;  min. 5765 Mbps;   * + Wymagana moc nadawania:   min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;  min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;  min. 22 dBm dla pasma 6GHz z możliwością zmiany co 1dBm   * + Wsparcie dla kanałów 20/40/80/160/320MHz,   + Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5dBi dla pasma 6GHz.   + Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy.   + Każdy z modułów radiowych musi posiadać możliwość pracy jako dedykowany skaner. * Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512 * Funkcje dodatkowe:   + OFDMA UL i DL   + Spatial Reuse (BSS Coloring)   + UL-MU-MIMO   + DL-MU-MIMO   + Enhanced Target Wake Time (TWT)   + Wbudowany analizator widma   + Wbudowane mechanizmy WIPS/WIDS   **- Gwarancja oraz wsparcie**  Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |

### Licencja na system uwierzytelniania, autoryzacji i kontroli dostępu 1 szt.

Oferowane rozwiązanie musi pozwalać na centralne zarządzenie kontami użytkowników oraz procesem uwierzytelnienia – w tym celu musi zapewniać wszystkie wymienione poniżej funkcje.

Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne, odpowiednio zabezpieczone systemy operacyjne dla poszczególnych komponentów.

|  |  |
| --- | --- |
| **Kategoria** | **Charakterystyka (wymagania minimalne)** |
| **Parametry systemu** | Poszczególne elementy wchodzące w skład systemu muszą zapewniać obsługę:   * 4 wirtualnych interfejsów sieciowych. * Możliwość uruchomienia w środowiskach: Microsoft Hyper-V Server 2016; VMware ESXi, ESX wersje:4,5,6; KVM, Xen, Microsoft Azure, AWS, Oracle OCI. |
| **Parametry wydajnościowe i licencyjne** | System musi obsługiwać co najmniej:   * Uwierzytelnianie dla 1100 użytkowników. * 200 tokenów dla uwierzytelniania dwuskładnikowego. * 30 klientów protokołu RADIUS (urządzeń NAS, które można podpiąć do systemu). * Możliwość zdefiniowania co najmniej 10 grup użytkowników, * 5 lokalnych centrów certyfikacji (CA).   Możliwość wygenerowania 5000 certyfikatów dla użytkowników. |
| **Wymagania ogólne** | System musi zapewniać nie mniej niż:   * Możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności. * Graficzną reprezentację statusu uwierzytelnionych użytkowników. * Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia oraz nazwą użytkownika:   + Lokalnie.   + Zdalnie w oparciu o protokół Syslog.   Konfigurację Captive Portalu. |
| **Wymagania funkcjonalne – uwierzytelnianie** | Celem realizacji funkcji uwierzytelniających, system musi zapewniać nie mniej niż:   * Lokalną, wbudowaną bazę użytkowników. * Przechowywanie następujących informacji o użytkowniku: nazwa, imię i nazwisko, adres email, numer telefonu, adres, kraj, województwo. * Możliwość zdefiniowania co najmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników. * Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV. * Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:   + poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych),   + czasu ważności hasła, * Konfigurowalną politykę blokowania kont, która będzie uwzględniać:   + ilość nieudanych logowań,   + czas blokowania konta,   + okres nieaktywności, po którym konto jest blokowane. * Możliwość odzyskiwania haseł:   + z wykorzystaniem adresu email,   + z wykorzystaniem pytania pomocniczego. * Obsługę protokołu RADIUS zgodną z RFC, w tym zakresie system musi oferować:   + wbudowany serwer RADIUS,   + integrację z zewnętrznymi serwerami RADIUS – praca jako klient. * Obsługę protokołu LDAP, w tym zakresie system musi oferować:   + wbudowany serwer LDAP,   + możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP). * Obsługę protokołu SAML - Identity Provider (IdP) proxy. * Realizację funkcji SSO (Single Sign On) w oparciu o:   + integrację z Active Directory, również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny,   + dedykowaną aplikację instalowaną na stacjach roboczych z systemem Windows,   + kontekst użytkownika przesyłany z serwera RADIUS,   + informacje uzyskiwane poprzez protokół Syslog, |
| **Wymagania funkcjonalne – uwierzytelnianie dwuskładnikowe** | Realizując uwierzytelnianie dwuskładnikowe, system musi zapewniać nie mniej niż:   * Obsługę dla tokenów sprzętowych (hardware):   + wspomniane tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania. * Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile. * Dla tokenów na system iOS i Android wymaga się:   + aktywacji z centralnego systemu uwierzytelniania (seed provisioning),   + możliwości konfiguracji ilości generowanych cyfr (6 lub 8),   + generowania kodu (cyfr) co 30 lub 60 sekund,   + możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne),   + ochrony dostępu poprzez konfigurowalny kod PIN,   Możliwość integracji z logowaniem do systemu Windows. |
| **Wymagania funkcjonalne – 802.1x** | System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki:   * Obsługa co najmniej poniższych protokołów EAP:   + PEAP,   + EAP-TTLS,   + EAP-TLS,   + EAP-GTC. * Wsparcie dla uwierzytelnienia w oparciu o adres MAC (MAC based authentication). * Zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTLS, TLS. |
| **Wymagania funkcjonalne – zarządzanie certyfikatami** | System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż:   * Obsługa wbudowanego CA (Certificate Authority). * Obsługa CA pośredniczących (Intermediate CA). * Ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego. * Możliwość pobrania wygenerowanych certyfikatów. * Możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP. * Możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP. * Możliwość generowania certyfikatów typu wildcard. * Realizacja CRL (Certificate Revocation List). * Wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560). * Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych. |
| **Zarządzanie** | * Zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki. * System udostępnia graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS. * Tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI) oraz na zewnętrzny serwer FTP/SFTP w oparciu o harmonogram, który będzie umożliwiał wskazanie konkretnego czasu kiedy proces ma się rozpocząć. * Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych. |
| **Serwis, wsparcie** | Wymaga się aby dostawa obejmowała również serwis producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. |

## Modernizacja sieci LAN

|  |
| --- |
| Przedmiotem zamówienia jest modernizacja oraz częściowa rozbudowa infrastruktury sieci lokalnej (LAN) w budynkach A i B szpitala, mająca na celu dostosowanie istniejącego okablowania strukturalnego do wyższych standardów transmisji danych oraz zapewnienie możliwości podłączania dodatkowych punktów sieciowych.  W ramach realizacji zamówienia Wykonawca zobowiązany jest do dostarczenia wszystkich materiałów, urządzeń i komponentów niezbędnych do prawidłowego wykonania prac objętych niniejszym opisem.  Zakres zamówienia  **1. Prace w punkcie dystrybucyjnym budynku A, obejmujące:**   * demontaż istniejących modułów sieciowych typu AMP ACO PLUS oraz montaż modułów typu keystone S/FTP spełniających standard kategorii 6A (Cat. 6A); wymianie podlega łącznie 145 modułów, * przełożenie istniejącego okablowania strukturalnego do innej szafy typu rack (bez dostawy nowej szafy rack), wraz z uporządkowaniem oraz oznaczeniem torów kablowych.   **2. Wymiana modułów sieciowych gniazd w części użytkowej budynku A, obejmująca:**   * demontaż istniejących modułów gniazd sieciowych typu AMP ACO PLUS oraz montaż nowych modułów sieciowych typu keystone S/FTP kategorii 6A (Cat. 6A), 145 gniazd sieciowych odpowiadającym torom kablowym zakończonym w punkcie dystrybucyjnym podlegającym modernizacji, * wymianę adapterów mocujących moduły na adaptery kompatybilne z istniejącymi ramkami ściennymi, przy zachowaniu istniejących ramek,   **3. Rozbudowa infrastruktury LAN w budynkach A i B, obejmująca:**   * wykonanie nowych punktów gniazd sieciowych wraz z niezbędnym okablowaniem strukturalnym – 24 gniazda z modułami keystone z zachowaniem standardu okablowania S/FTP kategorii 6A (Cat. 6A) * doprowadzenie kabli do właściwych punktów dystrybucyjnych dla danego budynku.   **4. Czynności towarzyszące:**   * wykonanie pomiarów i testów poprawności połączeń po zakończeniu prac, * opracowanie i przekazanie dokumentacji powykonawczej obejmującej aktualizację oznaczeń punktów logicznych.   **Wymagania organizacyjne**   * Prace muszą być realizowane w sposób zapewniający ciągłość funkcjonowania szpitala, z minimalizacją przerw w dostępie do sieci teleinformatycznej * Ze względu na charakter obiektu, Zamawiający wymaga prowadzenia prac w godzinach nocnych oraz w weekendy, a także etapowania robót i ich ścisłej koordynacji z przedstawicielami Zamawiającego. |

## Wdrożenie

|  |
| --- |
| W ramach wdrożenia Wykonawca musi zapewnić komplet kabli połączeniowych LAN/światłowodowych/DAC oraz modułów FC/SFP/SFP+/QSFP oraz innych akcesoriów niezbędnych dla zrealizowania w pełni działającego, maksymalnie wydajnego środowiska.  Zakres prac, które należy wykonać w ramach wdrożenia:   * instalacja i uruchomienie wszystkich dostarczonych urządzeń serwerowych/storage, * integracja dostarczonych urządzeń z infrastrukturą informatyczną Zamawiającego, * migracja środowiska informatycznego na nowe urządzenia zmiana wirtualizatora wiodącego dla środowiska IT * ⁠migracja maszyn wirtualnych, weryfikacja poprawności działania * migracja maszyn wirtualnych * optymalizacja działania zmodernizowanego środowiska IT * uruchomienie nowego środowiska bazy danych opartego o platformę OLVM zgodnie z licencjonowaniem Zamawiającego * migracja baz danych u Zamawiającego na nową infrastrukturę * optymalizacja i strojenie nowego środowiska bazy danych * uruchomienie i testy wdrożonego systemu kopii bezpieczeństwa * testy odtworzeniowe wdrożonego systemu kopii bezpieczeństwa * integracja na poziomie sprzętowym * implementacja dostępnych zabezpieczeń danych na poziomie sprzętowym * ⁠implementacja dostępnych integracji środowiska kopii zapasowych z dostarczonym sprzętem * uruchomienie nowego środowiska WiFi zgodnie z wymogami Zamawiającego * wymiana wszystkich punktów dostępowych na nowe z uwzględnieniem dostępności pomieszczeń ustalonej z Zamawiającym * wdrożenie dostępnych zabezpieczeń sieci WiFi, uruchomienie sieci dla gości zgodnie z aktualnie obowiązującymi * uruchomienie nowego środowiska sieciowego opartego o dostarczone przełączniki (TOR + Access) * optymalizacja dostarczonych przełączników klasy TOR pod kątem wydajności, bezpieczeństwa i wysokiej dostępności * ⁠optymalizacja dostarczonych przełączników klasy Access pod kątem wydajności i bezpieczeństwa dostępu użytkowników końcowych * Uruchomienie dostępnych mechanizmów zabezpieczeń zgodnie z wymogami Zamawiającego * migracja środowiska sieciowego (kablowego) na nowe urządzenia * wdrożenie i optymalizacja dostarczonych urządzeń klasy UTM do pracy na brzegu sieci zgodnie z wymaganiami Zamawiającego i aktualnie obowiązującymi standardami * ⁠optymalizacja zabezpieczeń sieci Zamawiającego w oparciu o dostępne oprogramowanie i urządzenia z zachowaniem tzw. najlepszych praktyk i standardów * uruchomienie systemów monitorowania pracy dostarczonych urządzeń i powiadamiania w razie wystąpienia awarii (możliwe wykorzystanie systemów na licencji Open Source) * uruchomienie systemów monitorowania pracy dostarczonych urządzeń i powiadamiania w razie wystąpienia awarii (możliwe wykorzystanie systemów na licencji Open Source) * wykonanie dokumentacji powdrożeniowej * zabezpieczenie sieci Zamawiającego w oparciu o dostarczone oprogramowanie i urządzenia |