Załącznik Nr 10 do SWZ

Powiat Warszawski Zachodni
ul. Poznańska 129/133
05-850 Ożarów Mazowiecki

OPIS PRZEDMIOTU ZAMÓWIENIA

NAZWA ZADANIA: **ZAKUP I DOSTAWA SPRZĘTU KOMPUTEROWEGO NA POTRZEBY STAROSTWA POWIATU WARSZAWSKIEGO ZACHODNIEGO**

Część 1 zamówienia – Poprawa cyberbezpieczeństwa w Starostwie Powiatu Warszawskiego Zachodniego – część I

NAZWY i KODY CPV:

30200000-1	-	Urządzenia komputerowe
30236000-2	-	Różny sprzęt komputerowy
30234600-4	-	Pamięć flash
48822000-6	-	Serwery komputerowe
48000000-8	-	Pakiety oprogramowania i systemy informatyczne
48700000-5	-	Pakiety oprogramowania do kopii zapasowych i odzyskiwania

1. Urządzenie UTM Fortigate-80F wraz z licencjami Unified Threat Protection (UTP) na 24 miesiące .

Dostawa urządzenia UTM Fortigate-80F wraz z licencjami Unified Threat Protection (UTP) na 24 miesiące, w celu zbudowania klastra wysokiej dostępności lub urządzenia równoważnego, które umożliwi utworzenie klastra z obecnie użytkowanym przez Zamawiającego urządzeniem Fortigate-80F

2. System kopii zapasowych

Dostawa subskrypcji oprogramowania do wykonywania kopii zapasowych

1.1 Wymagania ogólne

a. 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: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5.

b. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
c. Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.5.x - 6.7.x, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4 lub nowszy oraz Proxmox VE 8.2 lub nowszy.
d. 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.
e. Oprogramowanie musi być dostarczone w modelu oprogramowanie jako usługa – SaaS na okres 24 miesięcy.
f. Oprogramowanie musi umożliwiać wykonywanie kopii zapasowych z klastra wysokiej dostępności składającego się z 3 hostów fizycznych i 3 CPU (48 core) łącznie.
g. Oprogramowanie musi umożliwiać wykonywanie kopii zapasowych minimum 20 maszyn wirtualnych.

2.1 Całkowite koszty posiadania

a. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
b. Oprogramowanie musi tworzyć „samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
c. 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
d. 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.
e. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
f. 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.
g. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
h. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
i. 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)

j. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
k. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
l. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
m. 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
n. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
o. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
p. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
q. Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora)
r. Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS)
s. Oprogramowanie musi posiadać integracje z systemami typu SIEM
t. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.

3.1 Wymagania RPO (docelowy czas odzyskiwania)

a. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
b. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
c. 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 na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru
d. 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.
e. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
f. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).
g. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
h. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.

i. 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.
j. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
k. 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.
l. 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.
m. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
n. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
o. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

4.1 Wymagania RTO (docelowy punkt odzyskiwania)

a. 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.
b. 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)
c. 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
d. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
e. 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.
f. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
g. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
h. 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

i. 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.
j. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
k. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
l. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
m. 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.
n. 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.
o. 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.
p. 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.
q. 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.
r. 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.
s. Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
t. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
u. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
v. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

5.1 Ograniczenie ryzyka

a. 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)
b. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
c. 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

d. 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.
e. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware
f. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania
g. Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków
h. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

6.1 Środowiska fizyczne

a. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
b. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
c. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, Rocky Linux, AlmaLinux
d. Rozwiązanie musi wspierać system operacyjny macOS
e. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
f. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
g. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
h. 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
i. Rozwiązanie musi wspierać backup podłączonych dysków USB
j. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
k. 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)
l. Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
m. Rozwiązanie musi wspierać kontrolę pasma sieciowego
n. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych

o. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
p. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
q. Rozwiązanie musi wspierać technologię BitLocker
r. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
s. 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
t. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
u. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
v. 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
w. Rozwiązanie musi wspierać szyfrowanie
x. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
y. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
z. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
aa. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych

7.1 Monitoring

a. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
b. System musi umożliwiać monitorowanie 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
c. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
d. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
e. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
f. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
g. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
h. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora

i. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
j. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
k. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
l. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
m. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
n. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
o. 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.
p. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
q. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.6

8.1 Raportowanie

a. 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
b. System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
c. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
d. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
e. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
f. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
g. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
h. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
i. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
j. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
k. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury

l. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
m. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
n. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
o. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
p. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
q. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

3. Urządzenia serwerowe

Dostawa 3 szt. serwerów o poniższych parametrach minimalnych.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5” • Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania minimum jednego procesora. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych.
Procesor	• Zainstalowany jeden procesor 16-rdzeniowy klasy x86, min. 3.0GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 177 punktów w teście

	SPECrate2017_int_base dostępnym na stronie www.spec.org dla oferowanego serwera.
RAM	• Min. 256GB DDR5 RDIMM 5600MT/s
Zabezpieczenia pamięci RAM	• Memory demand and patrol scrubbing, • Failed DIMM isolation, • Memory address parity protection
Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10
Dyski twarde	• Zainstalowane: ○ 2x dysk SSD SATA o pojemności min. 480GB, 2,5“ Hot-Plug. • Możliwość zainstalowania dwóch dysków M.2 NVMe SSD Hot-Plug o pojemności min. 960GB z możliwością konfiguracji RAID 1.
Gniazda PCIe	• Trzy sloty PCIe
Interfejsy sieciowe/FC	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) • Dodatkowa, dwuportowa karta 10Gb Ethernet w standardzie BaseT

Wbudowane porty	• 4 porty USB w tym min:
	  ○ 1 port USB 3.0 z tyłu obudowy,
	  ○ 1 port micro USB z przodu obudowy
	• 2 port VGA z czego jeden z przodu obudowy
	• Możliwość rozbudowy o port RS232

Video	• Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200
Wentylatory	• Redundantne
Zasilacze	• Redundantne, Hot-Plug maksymalnie 1100W klasy Titanium
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
System operacyjny/dodatkowe oprogramowanie	• Windows Server 2022 Datacenter • Windows Server 2022 CAL per users 200 szt – licencje dostępowe przypisane do jednego z serwerów lub równomiernie do wszystkich.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.

	• Moduł TPM 2.0 V3 • 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 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800- 147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego, karta zarządzająca, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej; o zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); o szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; o możliwość podmontowania zdalnych wirtualnych napędów; o wirtualną konsolę z dostępem do myszy, klawiatury; o wsparcie dla IPv6; o wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; o integracja z Active Directory; o możliwość obsługi przez dwóch administratorów jednocześnie; o wsparcie dla dynamic DNS; o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. o możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera o możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: o Wirtualny schowek ułatwiający korzystanie z konsoli

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

	potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości

	przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory

	▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware o możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty o Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, o Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji o Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo o Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. o Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. o Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.

	○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android • Certyfikaty ○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami: ▪ ISO 27001 ▪ NIST Security and Privacy Controls for Federal Information Systems and Organization ▪ CSA Cloud Control Matrix
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły 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 - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.**

	• Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, 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 Producenta (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) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną

	diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: o Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. o Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. o Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. o Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. o Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

4. <u>Macierz</u>

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1	Sprzęt	Dostarczenie macierzy dyskowej umożliwiających pracę w trybie (synchronicznym/ asynchronicznym) Active/Active. Macierz musi być gotowa na pracę z drugą macierzą pomiędzy zdalnymi lokalizacjami (min.20 km) oraz szyfrowanie danych. Wyposażona w dwa kontrolery pracujące w trybie active/active w zakresie danych wejściowych, zamawiający dopuszcza tryb ALUA w przypadku zaoferowania rozwiązania z pamięcią cache min 512GB na kontroler. Tryb Active/Active nie może powodować obniżenia któregokolwiek z parametrów macierzy.
		Połączenia pomiędzy komponentami macierzy dyskowej muszą być realizowane w oparciu o technologię technologii PCIe lub NVMe.
		Macierz musi obsługiwać wyłącznie dyski typu NVMe niezależnie od skali systemu.
		Macierz musi być wyposażona w procesory wyposażone we wsparcie dla protokołu NVME. Zamawiający dopuszcza architekturę X86 dwóch producentów procesorów Intel (z generacją co najmniej Skylake) oraz AMD (z generacją Epyc).
		Oferowana macierz dyskowa musi posiadać minimum 192 GB pamięci cache na kontroler. Zamawiający nie dopuszcza możliwości zastosowania dysków SSD lub kart pamięci FLASH jako pamięci cache.
		Macierz musi posiadać dwa niezależne kontrolery z możliwością rozbudowy poprzez bezprzerwową wymianę kontrolerów do modelu wyższego. Proces wymiany nie może wymagać od zamawiającego okien serwisowych, producent musi zapewnić konsystencje danych w trakcie w.w procesu. Wydajność i pojemność takiej macierzy musi wówczas rosnąć liniowo. Zabrania

		się wykonywania ww. rozbudowy poprzez wymianę macierzy na model z innej rodziny produktowej.
		Macierz musi mieć możliwość zainstalowania w standardowej szafie serwerowej 19” lub musi być dostarczona z dedykowaną szafą umożliwiającą podłączenie do infrastruktury zamawiającego.
		Macierz dyskowa musi się cechować zużyciem energii poniżej 1 kWh na 3U rozmiaru fizycznego w szafie RACK.
2	Pojemność	Macierz musi gwarantować 24 TB przestrzeni z uwzględnieniem ochrony danych na poziomie RAID6 oraz mechanizmów deduplikacji oraz kompresji danych bez wykorzystania Thin Provisioningu.
		Macierz musi umożliwiać rozbudowę do konfiguracji gwarantującej przestrzeń RAW nie mniejszą niż 94 TB.
3	Wydajność	Oczekiwana wydajność to minimum 200 000 IOPS. Dla wydajności macierzy proszę przyjąć warunki: zapis/odczyt na poziomie 30/70, 100% losowo przy bloku 8kB, zerowych trafieniach w pamięć CACHE oraz przy dopuszczalnym średnim opóźnieniu max 0.4 ms. Wydajność jest liczona w obrębie dwóch kontrolerów, przy czym awaria kontrolera macierzy nie może powodować spadku wydajności systemu. Deduplikacja, kompresja, implementacja podwójnej parzystości, szyfrowanie wszystkich danych oraz uruchomione snapshoty nie mogą wpływać na wydajność macierzy.
4	Wysoka dostępność	Kontrolery muszą pracować w trybie wysokiej dostępności, tzn. w przypadku awarii jednego kontrolera, inny kontroler automatycznie przejmuje jego funkcje, czyli udostępnia klientom (tzw. hostom) wszystkie zdefiniowane w macierzy zasoby bez utraty połączenia do tych zasobów. Awaria kontrolera nie może powodować spadku wydajności macierzy w punktu widzenia hostów.

		Macierz będzie zasilana jednocześnie z dwóch niezależnych źródeł zasilania. Zanik jednego z nich nie może powodować przerwy w pracy urządzenia.
		Wszystkie krytyczne komponenty macierzy: kontrolery, zasilacze, wentylatory muszą pracować w trybie nadmiarowym, tak aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu.
		Możliwość uaktualniania oprogramowania (firmware'u) macierzy bez przerywania pracy systemu i bez przerwy w dostępie do danych od strony hostów oraz bez spadku wydajności w trakcie trwania w.w operacji.
		Macierz musi zapewniać poziom protekcji danych odpowiadający cechom RAID 6.
		W przypadku awarii dwóch dysków w grupie dyskowej odbudowa nie może mieć wpływu na wydajność systemu.
		Macierz musi wspierać obsługę wielu kanałów I/O (multipathing). W przypadku awarii ścieżki dostępu do macierzy musi nastąpić automatyczne przełączenie kanału komunikacji. Przełączanie kanałów I/O musi być wspierane przez natywne mechanizmy systemów operacyjnych wspieranych przez macierz.
5	Bezpieczeństwo danych	Macierze muszą realizować szyfrowanie danych algorytmem AES 256 lub lepszym – globalnie i domyślnie dla wszystkich danych zapisywanych na systemie. Dodatkowo macierz musi realizować szyfrowanie wszystkich zainstalowanych dysków. Oba niezależne klucze szyfrujące muszą być wymieniane domyślnie co 24h oraz po każdym zdarzeniu wyjęcia nośnika danych.
		Macierze mogą zostać zabezpieczone kluczem sprzętowym w celu zablokowania dostępu do danych na wypadek próby uruchomienia macierzy w sposób nieautoryzowany. Usunięcie klucza

		sprzętowego z macierzy uniemożliwia odczyt danych użytkownika.
		Macierz musi wspierać szyfrowanie dysków natywnie lub za pomocą dostarczonych narzędzi zewnętrznych bez wpływu na wydajność macierzy. a. Szyfrowanie powinno umożliwiać zabezpieczenie danych zgodnie z minimum FIPS 140-2. b. Produkt lub oprogramowanie do szyfrowania musi znajdować się na liście weryfikacji programu FIPS 140-3 https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/modules-in-process-list
		c. Wszystkie zasoby macierzy, w tym klony i kopie migawkowe (snapshoty), mogą być objęte konfigurowalną retencją danych o długości do 30 dni d. Usunięcie dowolnego zasobu, w tym klona czy migawki, nie oznacza jego skasowania przynajmniej na okres 24 godzin. e. Usunięte zasoby macierzy, w tym klony i migawki, mogą zostać przywrócone przez określony (konfigurowalny) czas. f. Ostateczne skasowanie dowolnego zasobu macierzy, w tym klona czy migawki, nie może odbyć się z pominięciem skonfigurowanego czasu retencji (np. od razu po jego usunięciu). g. Czas retencji może zostać skonfigurowany globalnie dla wszystkich zasobów i/lub za pomocą reguł dla wybranej grupy zasobów. h. Czas retencji może zostać zablokowany w taki sposób, aby administrator macierzy nie miał możliwości jego skrócenia niezależnie od poziomu jego uprawnień. i. Czas retencji może być zablokowany w taki sposób, aby administrator nie miał możliwości ostatecznego skasowania zasobów macierzy, w tym migawek czy klonów, przed upływem skonfigurowanego dla tych zasobów czasu retencji i niezależnie od poziomu uprawnień administracyjnych. j. Zapełnienie macierzy w 100% dostępnej pojemności nie może powodować utraty dostępu do danych. k. Analiza i ochrona wolumenów pod kątem ataków ransomware. l. Migawki i klony są zawsze oparte o wskaźniki (metadane) m. Wykonanie migawki dowolnego zasobu jest natychmiastowe i nie zajmuje dodatkowego miejsca na dane n. Wykonanie migawki nie inicjuje żadnego procesu kopiowania danych
		o. Dla zasobów replikowanych synchronicznie, polityka retencji danych również podlega replikacji i jest spójna dla obu

		macierzy biorących udział w relacji replikacji synchronicznej. p. Dla zasobów replikowanych asynchronicznie, polityka retencji danych może być skonfigurowana niezależnie dla źródła i celu w relacji replikacji. q. Dla zasobów klonowanych polityka retencji danych może być inna niż dla zasobów źródłowych.
		Uszkodzone dyski pozostają własnością Zamawiającego. Rozwiązanie równoważne – macierz szyfruje wszystkie dane i nośniki algorytmem minimum AES256 z wymianą kluczy szyfrujących domyślnie co 24h oraz po każdym zdarzeniu wyjęcia nośnika danych.
6	Protokoły Porty dostępowe	Macierz musi prezentować dane z użyciem iSCSI, NVMe-o-Fabric (TCP, FCP, RDMA) oraz natywnie realizować usługi plikowe dla protokołów NFS v3/v4 i SMB v2/v3
		Natywna obsługa protokołów NFS oraz SMB musi być realizowana w obrębie kontrolerów macierzy bez konieczności dodawania zewnętrznych głowic NAS lub wewnętrznego oprogramowania producentów innych niż producent macierzy np. w postaci kontenera, wirtualnej maszyny itp.
		Oprogramowanie macierzy musi realizować: a. Wsparcie dla wolumenów blokowych LUN min. 64TiB b. Wsparcie dla wolumenów Plikowych NAS CIFS/NFS min. 1PiB c. Obsługę minimum 5 miliardów plików per system
		Macierz musi posiadać możliwość podłączenia do sieci Ethernet co najmniej 4 portami SFP+ 10/25Gbps (wkładki światłowodowe obsługujące transfer 10Gbps wraz z patchcordami 3m lub kompatybilne przewody DAC+ 3m będą dołączone do macierzy).
7	Efektywność danych	a. Deduplikacja, kompresja oraz thin provisioning nie wymagają żadnej konfiguracji i są zawsze włączone oraz zachodzą dla wszystkich danych zapisywanych na macierzy w trybie in-line oraz post-process. b. Deduplikacja odbywa się zmiennym blokiem od 512B do 32KB – zamawiający dopuści rozwiązanie deduplikujące stałym blokiem w przypadku zaoferowania 2x większej pojemności

		netto tj. 44TB netto) c. Kompresja implementowana jest minimum 5 zmiennymi algorytmami. d. Deduplikacja, kompresja i thin provisioning nie wpływają na wydajność macierzy. e. Macierze raportują globalny współczynnik redukcji danych i jego zmiany w czasie. f. Raportowany współczynnik redukcji danych uwzględnia tylko dane użytkowe i nie obejmuje kopii migawkowych.
8	Kopie zapasowe	Macierz musi umożliwiać tworzenie snapshotów istniejących wolumenów (minimalna liczba snapshotów 100 tys). Migawki (snapshoty) mogą być tworzone w oparciu o harmonogramy, niezależnie, dla różnych grup zasobów wraz z konfigurowalną, automatyczną retencją.
		a. Migawki i klony są zawsze oparte o wskaźniki. b. Wykonanie migawki dowolnego zasobu jest natychmiastowe. c. Wykonanie migawki wielu zasobów jest natychmiastowe. d. Wykonanie migawki nie inicjuje żadnego procesu kopiowania danych. e. Wykonanie klona nie inicjuje żadnego procesu kopiowania danych. f. Odtworzenie danych z migawki nie inicjuje żadnego procesu kopiowania danych. g. Odtworzenie danych z klona nie inicjuje żadnego procesu kopiowania danych. h. Klonowanie zasobów jest natychmiastowe, niezależnie od rozmiaru oraz ilości klonowanych zasobów. i. Klonowaniu podlega również rozmiar wolumenu źródłowego. j. Wykonanie migawki na zasobach replikowanych synchronicznie odbywa się na obu macierzach jednocześnie i nie inicjuje żadnego procesu kopiowania danych. k. Odtworzenie z migawki zasobów replikowanych synchronicznie nie zaburza procesu replikacji synchronicznej i odbywa się w sposób natychmiastowy i niewymagający resynchronizacji danych. l. Po sklonowaniu zasobu (klon dostępny R/W), zasób źródłowy może być od razu usunięty. Usunięcie nie inicjuje żadnego procesu kopiowania danych. m. Migawki i klony w momencie utworzenia nie zajmują przestrzeni dyskowej (cienkie klony oraz cienkie migawki oparte o wskaźniki - pointers). n. Migawki mogą być tworzone w oparciu o harmonogramy, niezależnie, dla różnych grup zasobów wraz z konfigurowalną, automatyczną retencją. o. Przywrócenie wolumenu z migawki lub klona przywraca również rozmiar zapisany w klonie lub migawce. p. Tworzenie migawek lub klonów nie blokuje żadnych operacji

		administracyjnych na wolumenie (np. można zmienić rozmiar wolumenu pomimo istniejących migawek czy klonów tego wolumenu). q. Utworzenie klona nie tworzy żadnej relacji pomiędzy klonem a wolumenem źródłowym. r. Wydajność klona jest taka sama jak wolumenu źródłowego od razu po zainicjowaniu operacji klonowania. s. Klon jest dostępny dla hostów w trybie R/W od razu po zainicjowaniu operacji klonowania.
9	Replikacja synchroniczna	Macierz musi posiadać możliwość replikacji danych w trybie synchronicznym. Funkcjonalność replikacji musi spełniać następujące założenia: a. Parametry danego zasobu (rozmiar, nazwa) również podlegają replikacji. b. Migawki danego zasobu również podlegają replikacji synchronicznej. c. Zasoby replikowane synchronicznie mogą być replikowane również asynchronicznie (kaskadowo lub niezależnie) d. Klony dowolnych zasobów są automatycznie replikowane synchronicznie. e. Komunikacja z mediatorem (świadkiem, quorum) klastra odbywa się z użyciem protokołu TCP/IP (HTTPS), f. Zmiana mediatora (świadka) w relacji synchronicznej nie wymaga przerwania procesów replikacji danych. g. Replikacja może odbywać się z użyciem zarówno sieci IP lub FC. h. W przypadku awarii jednej z macierzy lub połączenia między macierzami mechanizm replikacji synchronicznej gwarantuje dostępność danych na co najmniej jednej macierzy. Przywrócenie połączenia automatycznie resynchronizuje dane i automatycznie przywraca dostęp do danych z obu macierzy jednocześnie – nie jest dozwolone wymaganie interwencji manualnej celem przywrócenia działania replikacji. i. Replikacja synchroniczna zasobów może być zamieniona na replikację asynchroniczną bez przerwania dostępu do danych. j. Replikacja asynchroniczna zasobów może być zamieniona na replikację synchroniczną bez przerwania dostępu do danych. k. Mediator w replikacji synchronicznej musi umożliwiać konfigurację usługi na minimum 2000 wolumenów. l. System musi wspierać RTT na poziomie min 10ms. umożliwiając replikację w mniej wydajnych sieciach
	Replikacja	

	asynchroniczna	a. Migawki mogą podlegać replikacji asynchronicznej niezależnie od innych mechanizmów replikacji danych. b. Replikacja asynchroniczna migawek zasobów replikowanych synchronicznie. c. Replikacja wg harmonogramu replikacji z konfigurowalną retencją, niezależnie, na macierzy źródłowej i docelowej. d. Replikacja dowolnego zasobu na inną macierz na życzenie.
	Replikacja semi-synchroniczna	a. Wbudowana w macierz jako natywna usługa replikacji b. Umożliwiająca replikowanie dużych zasobów danych bez wpływu na wydajność zasobów źródłowych c. Obsługa wolumenów Blokowych oraz Plikowych d. Mechanizm kontroli konsystencji oparty o Journal Log e. Możliwość pre-mapowania hostów z wolumenami zdalnymi f. Tolerancja dla dowolnej latencji i długości łącza
10	Kompatybilność	Macierz musi wspierać następujące najnowsze systemy operacyjne (tj wersje datowane na ostatnie 6 miesięcy) bez konieczności zakupu dodatkowego płatnego oprogramowania dla następujących platform operacyjnych: a. Windows Server b. Linux – CentOS, Ubuntu, RedHat c. Vmware
		System operacyjny macierzy musi się integrować z funkcjonalnością Veeam Backup and Recovery minimum v12 i być przez nią natywnie obsługiwany.
11	Zarządzanie	Macierz musi posiadać graficzny interfejs web umożliwiający zdalne zarządzanie macierzą.
		Macierzami można zarządzać z poziomu wbudowanego GUI(HTML5), CLI (SSH) oraz REST API bez konieczności użycia oprogramowania instalowanego poza macierzą. Dostęp do GUI i/lub CLI może zostać skonfigurowany z użyciem Active Directory. Dla CLI, dodatkowo, dostęp może odbywać się z użyciem kluczy SSH.

		Macierze posiadają REST API i CLI umożliwiające automatyzację jakichkolwiek funkcjonalności dostępnych w ramach macierzy, zgodnie ogólnie przyjętymi, najlepszymi praktykami w zakresie bezpieczeństwa tego typu operacji.
12	Monitorowanie	Macierz powinna być dostarczona z oprogramowaniem pozwalającym na ciągłe monitorowanie i raportowanie zasobów i wydajności.
		Obsługa Usługi Phonehome/Call home, za pomocą bezpiecznego kanału komunikacji (HTTPS oparty o SSL minimum 128 bit) między produktami macierzą a platformą analityczną, pozwalajaca na przesyłanie danych telemetrycznych i logów do chmury, gdzie są one przetwarzane na potrzeby analizy wsparcia oraz wykorzystywane przez różne interfejsy użytkownika.
		a. Macierze mają możliwość wysyłania telemetrii bezpośrednio do producenta z możliwością podglądu przez administratora, również danych historycznych. b. Macierze mają możliwość nawiązania zdalnej sesji VPN do centrum serwisowego w celu umożliwienia dostępu przez personel producenta. Funkcjonalność jest włączana lub wyłączana w dowolnej chwili przez administratora macierzy.
	Platforma monitoringu	Platforma Analityczna zarządzania oraz monitoringu pamięcią masową, która musi oferować szereg funkcji ułatwiających zarządzanie infrastrukturą pamięci masowej, takich jak: a. monitorowanie wydajności i stanu pamięci masowej w czasie rzeczywistym. Użytkownicy mogą śledzić wykorzystanie zasobów, wydajność i inne kluczowe wskaźniki. b. wykorzystanie narzędzi do planowania pojemności i wydajności, pozwalające na lepsze zarządzanie zasobami macierzowym oraz unikanie problemów związanych z przeciążeniem. c. Musi umożliwiać zarządzanie pamięcią masową na podstawie zdefiniowanych polityk, pozwalając na automatyzację i optymalizację operacji. d. Musi umożliwiać automatyczne rebalansowanie obciążeń i zarządzanie wieloma systemami pamięci masowej jako jedną spójną całość. e. Platforma musi umożliwiać monitoring bezpieczeństwa oprogramowania wraz z wykonywać zdalną bezprzerwową aktualizację oprogramowania oraz zabezpieczań macierzy na

		żądanie użytkownika bez ingerencji wsparcia technicznego.
		a. Ocena odporności danych, wybudowane narzędzie do śledzenia polityk adaptacji technologii ochrony danych, wraz ze wskaźnikiem oceny poziomu ochrony danych na skali od 0 do 5. b. Wykrywanie anomalii redukcji danych – musi zawierać funkcje analizy zmiany poziomu redukcji danych wraz z potencjalną identyfikacją ataku ransomware, wspomagając szybsze odzyskiwanie danych. c. Oznaczanie (tagowanie) zasobów, Musi umożliwiać użytkownikom kategoryzowanie zasobów, takich jak macierze, wolumeny czy inne urządzenia, za pomocą tagów. Tagi mogą być używane do raportowania, zarządzania cyklem życia, alertów, powiadomień, polityk bezpieczeństwa i ochrony. d. Platforma Analityczna umożliwia zarządzanie dostępem do funkcji za pomocą flag funkcji, co pozwala na kontrolowanie, które funkcje są dostępne dla określonych organizacji lub użytkowników.
		Wraz z macierzą musi zostać dostarczone oprogramowanie do analityki end-to-end środowiska Vmware vSphere Zamawiającego korzystającego z zasobów oferowanej macierzy. Oprogramowanie musi: a. być dostępne dla administratora poprzez przeglądarkę WWW b. Umożliwiać jednoczesną analizę co najmniej: pojedynczej maszyny wirtualnej, pojedynczego pliku VMDK, pojedynczego hosta ESXi, pojedynczego wolumenu macierzy c. raportować następujące metryki w formie numerycznej i graficznej a. IOPS b. Przepustowość na sekundę (MB/GB per second) c. Opóźnienie (latencję) w ms d. Obciążenie CPU i pamięci dla maszyn wirtualnych d. Wskazywać w formie graficznej korelację analizowanego komponentu z pozostałymi monitorowanymi komponentami środowiska Vmware. Komponentem jest VM, plik VMDK, host ESXi, wolumen macierzy, kontroler macierzy. e. Raportować powyższe metryki historycznie na co najmniej 7 dni wstecz Jeżeli do działania w/w oprogramowania wymagana jest licencja

		musi ona zostać dostarczona na pełną oferowaną pojemność macierzy ze wsparciem producenta na okres zgodny z gwarancją macierzy.
13	Gwarancja	Urządzenie musi być objęte gwarancją min. 3 lat 24/7 z NBD czasem wymiany uszkodzonych komponentów, niezależnie od ilości danych zapisanych na nośnikach półprzewodnikowych. Tryb gwarancji musi umożliwiać ciągłe rozszerzenie/przedłużenie gwarancji dla macierzy przez producenta. System musi umożliwiać bezprzewodową aktualizację oprogramowania oraz sprzętu do wyższych generacji w ramach usługi gwarancyjnej producenta. W ramach aktualizacji oprogramowania oraz wymiany sprzętu, nie może wystąpić konieczność ustawiania okien serwisowych, oznacza to że system powinien podczas prac aktualizacyjnych być w pełni dostępny, a prace te nie powinny wpływać na wydajność systemu.

5. Przełącznik sieciowy

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.

Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

- Ilość portów 24 porty SFP+ oraz 24 porty 10GBaseT niezależne
- Chłodzenie od przodu do tyłu obudowy
- Możliwość instalacji redundantnego zasilacza
- Tablica MAC min. 128K
- Tablica ARP/NDP min. 8K
- Bufor 56Mb
- MTBF min. 133176 godzin
- Wydajność min. 714 Mp/s
- Przepustowość min. 960 Gb/s
- Port USB
- Port miniUSB
- Port zarządzania Out-of-band;
- Web GUI

- HTTPs
- CLI
- Telnet
- SSH
- SNMP
- MIB RSPAN
- Radius
- TACACS+
- DiffServ
- Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
- IPv4/IPv6 Multicast filtering
- IGMPv3 MLDv2 Snooping
- ASM & SSM
- IGMPv1,v2 Querier
- Auto-VoIP
- Auto-iSCSI
- Policy-based routing (PBR)
- LLDP-MED
- Spanning Tree
- Green Ethernet
- STP
- MTP
- RSTP
- PV(R)STP
- BPDU/STRG Root Guard
- EEE (802.3az)
- GVRP/GMRP
- Q in Q,
- Private VLAN
- DOT1X
- MAB
- Captive Portal
- DHCP Snooping
- Dynamic ARP
- Inspection
- IP Source Guard
- CPU min 800 Mhz
- Min 1GB RAM
- Min 256MB Flash
- Min ilość obsługiwanych VLAN 4K
- DHCP Server min 2K rezerwacji
- sFlow
- Minimalna ilość przełączników w stosie: 8
- Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
- Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
- Non-stop forwarding (NSF)
- Distributed Link Aggregation (LAGs across the stack)
- Ilość interfejsów IP 128
- Double VLAN Tagging (QoQ)

- PIM-DM (Multicast Routing - dense mode)
- PIM-DM (IPv6)
- PIM-SM (Multicast Routing - sparse mode)
- PIM-SM (IPv6)
- RIPv2
- RFC 2328
- RFC 1583
- OSPFv3
- OSPFv2 min. sąsiadów 400
- OSPFv3 min. sąsiadów 400
- OSPFv3 min. sąsiadów na interfejs 100
- UDLD
- LLPF
- DHCPv6 Snooping
- wysyłanie alertów na email
- MMRP
- Ilość ACL min. 100
- Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu
- Zasilacz z certyfikatem 80+
- CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014,
- Class A, EN 61000-3-3:2013, EN 55024:2010
- VCCI : VCCI-CISPR 32:2016, Class A
- RCM: AS/NZS CISPR 32:2013 Class A
- FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014
- ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014
- BSMI: CNS 13438 Class A

6. Biblioteka sieciowa

Komponent	Minimalne wymagania
Obudowa i pojemność	Wysokość maksymalnie 1U do instalacji w szafie Rack. Co najmniej 9 slotów przeznaczonych na zestaw taśm.
Połączenie	Co najmniej 1 port SAS o przepustowości co najmniej 6Gb/s w standardzie umożliwiającym podłączenie serwerów wraz z kontrolerem SAS PCIe low profile do montażu w serwerze Zamawiającego.
Napęd	Wyposażony w co najmniej 1 sztukę napędu SAS LTO 8. W komplecie: • kabel SAS umożliwiający podłączenie biblioteki do serwera o dł. min. 2m • 10 taśm LTO-8 • • 1 taśma czyszcząca
Gwarancja	• 3 lata gwarancji producenta • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / 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 sie na inną formę. • 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. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. • Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu. • W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).