

SPECYFIKACJA TECHNICZNA ZAMÓWIENIA

1. NAZWA I ADRES ZAMAWIAJĄCEGO

Ośrodek Leczenia Kompleksowego sp. z o.o.

ul. Wrocławka 81

63-400 Ostrów Wielkopolski

KRS: 0000138495

NIP: 6222466050

Regon: 251544620

2. PRZEDMIOT ZAMÓWIENIA

Przedmiot zamówienia obejmuje: Zakup, dostawę i zainstalowanie jednej sztuki serwera backupowego wraz z oprogramowaniem serwerowym i backupowym oraz macierzą dyskową w związku z realizacją Przedsięwzięcia nr 015OW/3297/II/2024 pod nazwą Wsparcie podstawowej opieki zdrowotnej (POZ) FENX.06.01-IP.03-0001/23, realizowanego w ramach programu Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko 2021-2027, współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego, realizowanego na podstawie umowy nr FENX.06.01-IP.03-0001/23-00/1374/2024/17 zawartej w dniu 27.03.2024

	Serwer backupowy wraz z oprogramowaniem serwerowym i backupowym oraz macierzą dyskową – 1 szt.
Nazwa producenta:	
Model, typ, oprogramowanie:	

I.p.	Parametry techniczne aparatu	Charakterystyka (wymagania minimalne)	Parametr wymagany	Parametr oferowany TAK / NIE (wypełnia Wykonawca)
SERWER BACKUPOWY WRAZ Z OPROGRAMOWANIEM BACKUPOWYM				
1.	Obudowa	<ul style="list-style-type: none"> Obudowa Rack o wysokości max 2U z możliwością instalacji min. 24 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz opcjonalnym organizatorem do kabli. W chwili dostawy serwer musi mieć dostępnych 16 zatok na dyski. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne lub/i dedykowany przenośny panel operatora - serwer musi posiadać możliwość monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) nie dopuszcza się bezpośredniej komunikacji bezprzewodowej z procesorem serwisowym dopuszcza się wyłącznie połączenie bezpośrednie np. USB czy dedykowanego złącza diagnostycznego, procesory serwisowe z komunikacją bezprzewodową muszą mieć możliwość całkowitej dezaktywacji komunikacji radiowej 	TAK	
2.	Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.	TAK	
3.	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych	TAK	
4.	Procesor	Zainstalowany jeden procesor mające dokładnie 16-rdzeni, min. 3.6GHz, klasy x86 osiągające w teście Spec.org Int Rate 2017 wynik baseline min. 382pkt w konfiguracji dwuprocessorowej w zakresie tego samego typu serwera. Wynik dostępny na stronie https://spec.org .	TAK	

5.	RAM	Minimum 256GB DDR5 RDIMM w kościach min. 32GB 5600MHz, na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. Wymagane bezwzględnie jest optymalne obciążenie pamięci RAM. Obsadzone wszystkie kanały pamięci procesora. Sugerowane konfiguracje pamięci 8x 32GB. System musi mieć możliwość rozbudowy do 8 TB DDR5 3DS RDIMM lub 4TB DDR5 RDIMM.	TAK,	
6.	Zabezpieczenia pamięci RAM	<ul style="list-style-type: none"> • SDDC • ADDDC • Bounded Fault detection / correction • Memory mirroring • ECC detection/correction 	TAK	
7.	Gniazda PCI	Minimum cztery sloty PCIe, w tym min jeden x16, oraz dwa x8 - PCIe5.0. Poza gniazdami PCIe dodatkowy sloty OCP 3.0 PCIe5.0 x16. Możliwość rozbudowy serwera do konfiguracji z min 12 slotami PCI i slotem OCP.	TAK	
8.	Interfejsy sieciowe/FC/SAS	min. 4 interfejsy sieciowe 1Gb (karta typu OCP) RJ45. dwa porty 10/25Gb SFP28.	TAK	
9.	Dyski twarde	Zainstalowane min. szesnaście dysków hotswap 2.5" 3.2TB MU SAS SSD lub NVMe. Zainstalowane dwa dyski na system operacyjny – m.2 SATA 6Gb 960GB RI pracujące w sprzętowym RAID1.	TAK	
10.	Kontroler RAID	Kontroler obsługujący do 16 dysków SAS/SATA/SSD z pamięcią cache min. 8GB.	TAK	
11.	Wbudowane porty	<ul style="list-style-type: none"> • Min 2x USB 3.0, opcjonalny port mini displayport dostępny z przodu serwera. Dedykowany port do zarządzania i diagnostyki dostępny z przodu serwera. • Min 2x USB 3.2, VGA port, RJ45 dla procesora serwisowego dostępny z tyłu serwera • Min 1x USB 3.2 dostępny wewnątrz serwera 	TAK	
12.	Video	Zintegrowana karta graficzna z wbudowaną dedykowaną pamięcią min 16MB, umożliwiającą wyświetlenie rozdzielczości min. 1920x1200 przy częstotliwości odświeżania min 60Hz	TAK	
13.	Wentylatory	Redundantne, Hot-Swap, posiadające redundantne silniki w każdym wentylatorze. Z uwagi na wysokie TDP procesorów muszą osiągać prędkość min. 17k obrotów / minutę.		

		Gwarancja poprawnego działania serwera nawet w temp. 30st C.		
14.	Zasilacze	Redundantne, Hot-Swap min. 1800W każdy. Posiadające certyfikat 80Plus Titanium.		
15.	Bezpieczeństwo	<ul style="list-style-type: none"> • panel zamykany na klucz służący do ochrony nieautoryzowanego dostępu do dysków twardej. • Opcjonalny czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Power-ON-Password oraz hasło administracyjne dla BIOS/UEFI • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane zdalnie poprzez dostarczone oprogramowanie zarządzające 		
16.	Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy lub dołączany poprzez dedykowany port, umożliwiający wyświetlenie informacji o stanie serwera		
17.	Karta Zarządzania	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:</p> <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalny dostęp poprzez SSH do CLI procesora serwisowego • obsługa IPMI 2.0, SNMP v3/v1, CIM-XML, DCMI 1.5, Redfish DMTF • przekierowanie portu szeregowego przez IPMI oraz SSH • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, temperatury: Otoczenia, CPU, pamięci DIMM); • Out-of-Band (OOB) monitorowanie obciążenia CPU/Pamięci/IO oraz całego systemu • szyfrowane połączenie (TLS min TLS 1.2) oraz autentykację i autoryzację użytkownika; • możliwość zamontowania zdalnych wirtualnych napędów, (obrazy ISO) minimum 4 obrazy iso jednocześnie w czasie jednej sesji • możliwość montowania obrazów ISO z lokalnej stacji zarządzającej poprzez przeglądarkę oraz poprzez współdzielone zasoby sieciowe min NFS/CIFS/HTTPS 		

		<ul style="list-style-type: none"> • wirtualną konsolę z dostępem do myszy, klawiatury; • wirtualna konsola oraz montowanie obrazów ISO bez instalacji dodatkowych komponentów Java czy AciveX (musi działać w oparciu o HTML5) • wsparcie dla IPv6; • wsparcie dla; SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym oraz historycznym min 24h poboru mocy oraz temperatur w serwerze; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory • możliwość zdefiniowania min 12 użytkowników lokalnych na karcie zarządzającej • możliwość obsługi zdalnej konsoli przez minimum czterech administratorów jednocześnie; • wsparcie dla dynamic DNS; • możliwość podglądu stanu serwera poprzez port USB i aplikację na urządzenie mobilne Android/iOS 		
18.	Oprogramowanie do zarządzania	<p>Dostarczone dodatkowe oprogramowanie producenta do zarządzania, spełniającego poniższe wymagania:</p> <ul style="list-style-type: none"> • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta w systemie operacyjnym • Automatyczne rozpoznawanie nowych serwerów poprzez protokół SLP oraz SSDP • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu danych min do formatu CSV • Grupowanie urządzeń w oparciu o kryteria użytkownika • Możliwość wizualizacji rozmieszczenia serwerów i zarządzanych urządzeń w szafach RACK • Tworzenie automatycznie grup urządzeń w oparciu o elementy konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji czy stanu np. firmware czy BIOS • Szybki podgląd stanu środowiska 		

	<ul style="list-style-type: none">• Podsumowanie stanu dla każdego urządzenia• Szczegółowy status urządzenia/elementu/komponentu• Filtry raportów umożliwiające podgląd najważniejszych zdarzeń• Integracja z service desk producenta dostarczonej platformy sprzętowej, pozwalając min weryfikacje statusu i dosyłanie paczek diagnostycznych• Możliwość przejęcia zdalnego pulpitu• Możliwość zamontowania wirtualnego napędu• Kreator umożliwiający dostosowanie akcji dla wybranych alertów• Przesyłanie alertów „as-is” do innych konsol firm trzecich• Możliwość definiowania ról administratorów• Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów• Aktualizacja oparta o repozytorium aktualizacji – budowanie repozytorium w sposób automatyczny ze stron producenta• Możliwość definiowania polityk aktualizacji (konkretne wersje firmware)• Automatyczna polityka aktualizacji „Najnowsze dostępne”• Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta na systemie operacyjnym• Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów• Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta• Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności czy powielania konfiguracji na inne serwery czy backup aktualnej konfiguracji.• Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile – opcja• Wykonanie restartu serwera i automatyczne wejście do BIOSu/UEFI• Zdalne bezpieczne usunięcie danych na dyskach SSD/HDD w serwerach		
--	--	--	--

		<ul style="list-style-type: none"> • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. • Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin: <ul style="list-style-type: none"> ○ wykonać zautomatyzowaną aktualizację firmware serwerów w klustrze Vmware do zdefiniowanej polityki poziomu mikrokodów ○ wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityką konfiguracji ○ z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny) ○ z konsoli vCenter uruchomić ○ inwentaryzacja komponentów w serwerze i ich mikrokodów ○ historia min 24h poboru mocy i temperatury serwera ○ zbieranie danych diagnostycznych serwera do paczki • Integracja z środowiskiem Microsoft Admin Center pozwalająca z konsoli/plugin: <ul style="list-style-type: none"> ○ wykonać zautomatyzowaną aktualizację firmware serwerów w klustrze do zdefiniowanej polityki poziomu mikrokodów ○ z konsoli Admin Center uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny) ○ aktualizacja sterowników systemowych Windows ○ inwentaryzacja komponentów w serwerze i ich mikrokodów ○ historia min 24h poboru mocy i temperatury serwera ○ zbieranie danych diagnostycznych serwera do paczki • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. 		
19.	Certyfikaty	<ul style="list-style-type: none"> • Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklarację CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok 		

		<p>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 Bronze według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu.</p> <ul style="list-style-type: none"> • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Windows 2025. 		
20.	Dokumentacja użytkownika	<ul style="list-style-type: none"> • 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. 		
21.	Warunki gwarancji	<ul style="list-style-type: none"> • 5 lat gwarancji producenta, wraz z usługą pozostawiania dysków. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie NBD następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz 		

		<p>pobieranie uaktualnień mikro kodu oraz sterowników.</p> <ul style="list-style-type: none"> Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Opcja rozszerzenia do poziomu usługi serwisowej gwarantującej 24 godzinny czas naprawy sprzętu od momentu rozpoznania problemu. 		
22.	Oprogramowanie	<p>Dołączone licencje oprogramowania Windows Server Standard 2025 na wszystkie zainstalowane rdzenie, z opcją downgrade do Windows 2022 i 2019. Wersja OEM. Dołączone 20 szt. licencji dostępowych CAL na urządzenie do oprogramowania Windows Server Standard 2025</p>		
MACIERZ DYSKOWA				
23.	Obudowa	<p>Macierz musi być dostarczona ze wszystkimi komponentami do instalacji w szafie rack 19".</p>	TAK	
24.	Pojemność:	<ul style="list-style-type: none"> Macierz musi zostać dostarczona w konfiguracji zawierającej minimum: 22 dysków NVME o pojemności minimum 3.8TB każdy Macierz musi wspierać dyski: <ul style="list-style-type: none"> SSD: 1.9TB, 3.8TB, 7.6TB, 15.3TB, przynajmniej jeden typ dysków musi mieć możliwość szyfrowania (FIPS) Macierz musi mieć możliwość rozbudowy do minimum 120 dysków hot-swap. Macierz musi być macierzą all-flash, nie dopuszcza się macierzy, która może jednocześnie obsługiwać dyski SSD i HDD. 	TAK	
25.	Kontroler	<p>Dwa kontrolery macierzy wyposażone w przynajmniej 32GB cache każdy (16GB na całą macierz). W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub</p>	TAK	

		jako zrzut na pamięć flash. Zawartość cache musi być mirrorowana (kopia lustrzana) między kontrolerami.		
26.	Interfejsy	<p>Oferowana macierz musi posiadać min. 8 portów 10/25Gb SFP28.</p> <p>Możliwość wymiany ww. portów na:</p> <ul style="list-style-type: none"> • 8 portów 16/32Gb FC obsadzonych wkładkami SFP+ • 4 porty 100Gb NVMe Over Roce <p>W standardzie muszą być też dostępne:</p> <ul style="list-style-type: none"> • 8 portów SAS 12 Gb/s do komunikacji z półkami rozszerzeń • 2 porty RJ-45 10/100/1000 Mb Ethernet typu out-of-band management. 	TAK	
27.	RAID	Kontrolery macierzy muszą umożliwiać konfigurację dysków w RAID: 0, 1, 3, 5, 6, 10. Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum 120 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych.	TAK	
28.	Obsługiwane protokoły	Macierz musi obsługiwać protokoły FC, iSCSI, iSER/IB, NVMe/FC, NVMe/RoCE, SRP/IB	TAK	
29.	Inne wymagania	<ul style="list-style-type: none"> • Macierz musi posiadać wsparcie dla systemów: <ul style="list-style-type: none"> ○ Microsoft Windows Server, Red Hat Enterprise Linux (RHEL); SUSE Linux Enterprise Server (SLES); VMware vSphere • Macierz musi posiadać funkcjonalność wykonywania minimum 1024 kopii migawkowych typu copy-on-write. Macierz musi posiadać funkcjonalność klonowania danych i replikacji asynchronicznej. • Macierz musi mieć możliwość replikacji danych po FC oraz iSCSI w trybie asynchronicznym. • Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie. • Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy, na których rezydują osobne dyski logiczne 	TAK	

		<p>dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 512 partycji.</p> <ul style="list-style-type: none"> • Macierz musi pochodzić od tego samego producenta co serwery rack objęte niniejszym zapytaniem. • Macierz musi posiadać funkcjonalność thin provisioning. • Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID. • Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji. • Macierz musi posiadać oprogramowanie pozwalające na integrację z VMware vCenter. • Macierz musi zapewniać możliwość szyfrowania danych przy użyciu dysków typu FIPS SSD. Realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami. 		
30.	Gwarancja i serwis	<ul style="list-style-type: none"> • 5 lat serwisu producenta. Wymagana jest naprawa w trybie NBD. • Dyski uszkodzone pozostają u Zamawiającego. • Dostarczony system musi posiadać również 5 lat subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia. • Opcja rozszerzenia do poziomu usługi serwisowej gwarantującej 24 godzinny czas naprawy sprzętu od momentu rozpoznania problemu. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. 	TAK	
OPROGRAMOWANIE DO BACKUPU				
31.	Funkcjonalność / wymagania ogólne	<ul style="list-style-type: none"> • 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 	TAK	

		<p>dostępnej liście referencyjnej Gartner Peer Insights: i spełniać minimalne wymaganie:</p> <ul style="list-style-type: none"> ○ minimalna liczba referencji 150, ○ minimalna ocena z referencji 4,5, ● Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 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 		
32.	<p>Funkcjonalność / całkowite koszty posiadania</p>	<ul style="list-style-type: none"> ● 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 	TAK	

		<p>co najmniej trzech pamięci masowych to takiej puli.</p> <ul style="list-style-type: none">• 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 jakiegokolwiek funkcjonalności wymienionej w tej specyfikacji• Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania	
--	--	--	--

		<ul style="list-style-type: none"> • 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. 		
33.	Funkcjonalność / wymagania RPO	<ul style="list-style-type: none"> • 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 conajmniej 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. 	TAK	

		<ul style="list-style-type: none"> • 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 punktu 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) 		
--	--	---	--	--

34.	Funkcjonalność / wymagania RTO	<ul style="list-style-type: none"> • Oprogramowanie musi umożliwić 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 uruchomienie 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 vSpehre • 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 	TAK	
-----	---------------------------------------	---	-----	--

	<ul style="list-style-type: none">• 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, enterprise 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		
--	--	--	--

		<p>odtworzenie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.</p> <ul style="list-style-type: none"> • 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 		
35.	<p>Funkcjonalność / ograniczenie ryzyka</p>	<ul style="list-style-type: none"> • 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 uruchomienie 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 	TAK	

		<p>na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem</p> <ul style="list-style-type: none"> • 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 hakeraśkiego 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 		
36.	Funkcjonalność / środowiska fizyczne	<ul style="list-style-type: none"> • 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 	TAK	

		<p>Linux, SLES, Fedora, openSUSE, Rocky Linux, AlmaLinux</p> <ul style="list-style-type: none"> • 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 deduplikację 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 		
--	--	--	--	--

		<p>bloków dla systemów serwerowych musi być certyfikowana przez Microsoft</p> <ul style="list-style-type: none"> • Rozwiązanie musi wspierać technologię BitLocker • Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania • Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednorazowej 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 zabezpieczonego • Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej • Rozwiązanie musi wspierać tworzenie wielu zadań backupowych 		
37.	Funkcjonalność / monitoring	<ul style="list-style-type: none"> • System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich 	TAK	

		<ul style="list-style-type: none">• 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• System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 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 kategoryzację 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		
--	--	---	--	--

		<ul style="list-style-type: none"> • 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 nadanych użytkownikom dla platformy VMware 		
38.	Funkcjonalność / raportowanie	<ul style="list-style-type: none"> • 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 2012, 2012R2, 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 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 	TAK	

		<ul style="list-style-type: none"> • 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 		
	<p>Rodzaj licencji</p>	<p>Licencja wieczysta</p>	<p>TAK</p>	

	Gwarancja i serwis	Wsparcie techniczne producenta na okres minimum 12 miesięcy	TAK	
INSTALACJA				
1.	Zakres	<ol style="list-style-type: none"> 1. Montaż dostarczonego sprzętu w szafie przemysłowej rack 2. Podłączenie serwera i macierzy dyskowej do infrastruktury Zamawiającego 3. Instalacja systemu Windows na nowym serwerze. 4. Konfiguracja roli Hyper-V 5. Inicjalizacja macierzy dyskowej 6. Podłączenie nowo utworzonych woluminów do serwera 7. Instalacja wirtualnego systemu operacyjnego Windows Serwer jako primary domain controller 8. Instalacja wirtualnego systemu operacyjnego Windows Serwer jako secondary domain controller 9. Instalacja wirtualnego systemu operacyjnego Windows Serwer 2022/2025 na potrzeby systemu backupu 10. Wprowadzenia do administracji systemem backupu – stworzenie przykładowego zadania backupu / odtworzenia. 	TAK	

.....
miejscowość i data

.....
(podpis osoby upoważnionej i pieczęć)