1. Serwer rack – 8 szt.

Lp.	Specyfikacja techniczna	
1.	**Obudowa**	a) Obudowa rack o wysokości max. 2U z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych wraz z ramieniem do mocowania kabli. b) Czujnik otwarcia obudowy współpracujący z BIOS/UEFI. c) Zdejmowany panel przedni z możliwością dodania zamka chroniącego przed nieuprawionym dostępem do dysków.
2.	**Płyta główna**	a) Dwuprocesorowa płyta zaprojektowana przez producenta serwera z możliwością instalacji procesorów 160 rdzeniowych i mocy 390W. b) Modułu TPM min. 2.0
3.	**Procesor**	Zainstalowane dwa procesory min. 32-rdzeniowe klasy x86 z częstotliwością bazową min. 3.55 GHz
4.	**Pamięć operacyjna**	a) Zainstalowane minimum 1TB pamięci RAM typu DDR5 Registered, 6400MT/s w modułach dwubankowych o pojemności 128GB każdy. b) Płyta główna z 24 slotami na pamięć i umożliwiająca instalację 6TB przy zastosowaniu odpowiednich pamięci. c) Wsparcie dla technologii zabezpieczania pamięci, min. Advanced ECC.
5.	**Sloty rozszerzeń**	a) Serwer musi być wyposażony w 4 aktywne slotów PCIe Gen5 x16 (bus width) gotowe do obsadzenia kartami. Dwa sloty muszą być wolne pod przyszłą rozbudowę.
6.	**Dyski M.2**	Zainstalowane dwa dyskami 480GB NVMe M.2 każdy w trybie hot-plug skonfigurowane fabrycznie w RAID1 umieszczone z tyłu serwera.
7.	**Kontroler**	Sprzętowy kontroler dyskowy z pojemnością cache minimum 8GB, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10. 50, 60, non-RAID (JBOD)
8.	**Interfejsy sieciowe**	a) Zainstalowane dwie dwuportowe karty sieciowe 10/25 Gbit/s SFP28 z certyfikowanymi przez producenta wkładkami 10Gb SR, przy czym co najmniej jedna z nich musi być zainstalowana w dedykowanym złączu sieciowym (np OCP 3.0) niezajmującym standardowych slotów PCIe, a druga może zająć standardowy slot PCIe. Zainstalowana trzecia dwuportowa karta sieciowa 10/25 Gbit/s SFP28 z wkładkami 25Gb SR z wkładkami zgodnymi i certyfikowanymi do pracy z oferowanym serwerem oraz objętymi wsparciem producenta serwera. b) Zainstalowana czteroportowa karta 1Gbit/s BASE-T. c) Dedykowany port 1Gb RJ45 dla karty zarządzającej.
9.	**Karta graficzna**	Zintegrowana karta graficzna
10.	**Porty**	a) Złącza USB: min. 3 portów min. USB 3.1 , min. 1 port z przodu obudowy b) Port video (VGA lub HDMI) z przodu serwera bez użycia zewnętrznych przejściówek na kablu USB
11.	**Zasilacze, chłodzenie**	a) Redundantne zasilacze typu hot-plug o sprawności 96% (tzw. klasa Titanium) i mocy min. 1800W każdy.

		b) Redundantny zestaw wentylatorów typu hot-plug min. 6 szt.
12.	**Diagnostyka**	Wbudowany mechanizm szybkiej diagnostyki pozwalający na weryfikację i odczyt stanu podzespołów z przodu obudowy.
13.	**Karta /moduł zarządzający**	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w gnieździe PCI posiadająca funkcjonalności: a) monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe dyski(fizyczne i logiczne) b) wsparcie dla pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z c) generowaniem alertów SNMP d) dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub przez współdzielony port zintegrowanej karty sieciowej serwera e) dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) f) wbudowane narzędzia diagnostyczne g) zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego h) wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników · przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) i) obsługa zdalnego serwera logowania (remote syslog) j) wirtualna zdalna konsola, tekstowa i graficzna z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD/CD/DVD. k) mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie l) monitorowanie zasilania oraz zużycia energii przez serwer w czasie z możliwością graficznej prezentacji m) konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) n) zdalna aktualizacja oprogramowania (firmware) o) zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power caping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy p) możliwość równoczesnej obsługi przez min. 2 administratorów q) autentykacja dwuskładnikowa (Kerberos) r) wsparcie dla Microsoft Active Directory s) obsługa TLS i SSH

		t) możliwość trwałego zablokowania dokonania obniżenia wersji oprogramowania układowego (firmware) serwera u) wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API v) możliwość autokonfiguracji sieci karty zarządzającej(DNS/DHCP).
14.	**Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych**	a) Microsoft Windows Server, min. 2022, 2025 b) Red Hat Enterprise Linux (RHEL), min. 8, 9, 10 c) SUSE Linux Enterprise Server (SLES), min. 15 d) VMware ESXi, min. 7, 8, 9 e) Oracle Linux, min. 9 Oferowany serwer musi znajdować się na liście VMware HCL dla ESXi 8, 9 oraz na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows 2022, 2025.
15.	**Kable**	a) 2 kable zasilające, min. 2m b) 6 kabli światłowodowych LC-LC multi-mode OM4, min. 2m
16.	**Gwarancja producenta**	a) min 36miesięczna gwarancja producenta z serwisem gwarancyjnym w miejscu instalacji przez inżyniera z czasem reakcji w następnym dniu rocznym (NBD). b) uszkodzone dyski pozostają u zamawiającego.

2. Wkładki światłowodowe, moduły i kable połączeniowe do posiadanych przełączników HPE 5945 4-slot Switch – JQ076A

Lp.	Specyfikacja techniczna	
1.	**Wkładki**	a) 20 wkładek światłowodowych HPE Networking X190 25G SFP28 LC SR 100m MM Transceiver -JL293A b) 2 moduły HPE Networking 5950 24p SFP28 and 2p QSFP28 Module - JH450A
2.	**Kable**	c) 40 kabli światłowodowych LC-LC multi-mode OM4, min. 2m
3.	**Gwarancja producenta**	min. 12 miesięczna gwarancja producenta przełączników

3. Macierze - 2 szt.

Lp.	Specyfikacja techniczna	
		Macierz musi posiadać dwa niezależne kontrolery z możliwością rozbudowy poprzez bezprzerwową wymianę kontrolerów do modelu wyższego.
		Macierz musi mieć możliwość zainstalowania w standardowej szafie serwerowej 19"

		Macierz dyskowa musi się cechować zużyciem energii poniżej 1.3 kWh na 3U rozmiaru fizycznego w szafie RACK.
2	Pojemność	Macierz musi gwarantować min. 100 TB przestrzeni RAW i jednocześnie min. 100 TiB z uwzględnieniem ochrony danych na poziomie RAID6 bez mechanizmów deduplikacji oraz kompresji danych bez wykorzystania Thin Provisioningu. Macierz ma zapewniać możliwość rozbudowy do przestrzeni min. 450 TB przestrzeni RAW bez wymiany zainstalowanych modułów dyskowych i montażu dodatkowych półek dyskowych,
3	Wydajność	minimum 300k IOPS. Dla wydajności macierzy proszę przyjąć warunki: zapis/odczyt na poziomie 70/30, 100% losowo przy bloku 8kB, zerowych trafieniach w pamięć CACHE oraz przy dopuszczalnym opóźnieniu nie wyższym niż 2ms 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.
		Macierz musi zapewniać poziom protekcji danych odpowiadający cechom RAID 6.
		Macierz musi wspierać obsługę wielu kanałów I/O (multipathing).
5	Bezpieczeństwo danych	Macierze muszą realizować szyfrowanie danych algorytmem co najmniej AES 256– 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. Wszystkie zasoby macierzy (plikowe oraz blokowe), w tym klony i kopie migawkowe (snapshoty), mogą być objęte konfigurowalną retencją danych o długości do 30 dni c. Usunięcie dowolnego zasobu, w tym klona czy migawki, nie oznacza jego skasowania przynajmniej na okres 24 godzin.

		d. Usunięte zasoby macierzy, w tym klony i migawki, mogą zostać przywrócone przez określony (konfigurowalny) czas. e. 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). f. Czas retencji może zostać skonfigurowany globalnie dla wszystkich zasobów i/lub za pomocą reguł dla wybranej grupy zasobów. g. Czas retencji może zostać zablokowany w taki sposób, aby administrator macierzy nie miał możliwości jego skrócenia niezależnie od poziomu jego uprawnień. h. 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. i. Zapełnienie macierzy w 100% dostępnej pojemności nie może powodować utraty dostępu do danych. j. Analiza i ochrona wolumenów pod kątem ataków ransomware. k. Migawki i klony są zawsze oparte o wskaźniki (metadane) l. Wykonanie migawki dowolnego zasobu jest natychmiastowe i nie zajmuje dodatkowego miejsca na dane m. Wykonanie migawki nie inicjuje żadnego procesu kopiowania danych
		n. Dla zasobów replikowanych synchronicznie, polityka retencji danych również podlega replikacji i jest spójna dla obu macierzy biorących udział w relacji replikacji synchronicznej. o. Dla zasobów replikowanych asynchronicznie, polityka retencji danych może być skonfigurowana niezależnie dla źródła i celu w relacji replikacji. p. Dla zasobów klonowanych polityka retencji danych może być inna niż dla zasobów źródłowych.
6	Protokoły Porty dostępowe	Macierz musi umożliwiać prezentowanie danych z użyciem FC 32/64Gb, iSCSI, NVMe-o-Fabric (TCP, FCP, RDMA) oraz natywnie realizować usługi plikowe dla protokołów NFS v3/v4 i SMB v2/v3 Wraz z macierzą musi być dostarczone 8 portów 10/25Gbit/s z wkładkami 25Gbit/s SFP+ Multi Mode.
		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.256TiB b. Wsparcie dla wolumenów plikowych NAS CIFS/NFS min. 1PiB c. Obsługę minimum 5 miliardów plików per system
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. c. Kompresja implementowana w trybie online 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 200 tys). Migawki (snapshoty) mogą być tworzone w oparciu o harmonogramy, niezależnie, dla różnych grup zasobów wraz z konfigurowalną, automatyczną retencją.

		Możliwość wykonania 2 tyś. snapshotów na każdym wolumenie bez konieczności tworzenia kopii lub klona.
		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 jak i 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 g. Replikacja wykonywana po protokole FC w topologii Uniform oraz Non-Uniform h. Replikacja musi wspierać Vmware vVOL
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 umożliwiać integrację z Vmware vSphere poprzez instalację wtyczki (pluginu) do Vmware vCenter, Vmware vRealize (Orchestrator oraz Operations Manager) oraz VM Log Insight. Wymienione aplikacje muszą rozpoznawać natywnie oferowaną macierz oraz intepretować jej statystyki.
11	Zarządzanie	Macierz musi posiadać graficzny interfejs web umożliwiający zdalne zarządzanie macierzą oraz wieloma macierzami.
		Macierzami można zarządzać z poziomu wbudowanego GUI(HTML5), CLI (SSH) oraz REST API bez konieczności użycia oprogramowania instalowanego poza macierzą.
		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.
		Interfejs musi umożliwiać zarządzanie od 1 do min. 50 macierzy poprzez pojedynczy wbudowany interfejs GUI(HTML5), CLI (SSH) oraz REST API bez konieczności użycia oprogramowania instalowanego poza macierzą. Interfejs musi umożliwiać tworzenie globalnych polityk bezpieczeństwa, replikacji oraz dostępu do danych, z którejkolwiek macierzy będącej w zbiorze.
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

	Platforma monitoringu	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 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. e. Platforma Analityczna musi umożliwiać tworzenie oraz wykonanie planu aktualizacji oprogramowania bez konieczności angażowania wsparcia technicznego. Aktualizacja powinna automatycznie sprawdzać obecny stan konfigurację macierzy, budować plan aktualizacji oraz zdalnie wywoływać aktualizację oprogramowania, bez konieczności interakcji z użytkownikiem oraz supportem. f. Automatyczna aktualizacja musi pozwalać na zatrzymanie oraz weryfikację procesu pomiędzy każdym z wcześniej zaplanowanych kroków. g. Platforma musi posiadać udokumentowane Rest API umożliwiające integrację z platformami zewnętrznymi.
		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	min. 36 miesięcy gwarancji 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. Uszkodzone dyski pozostają u zamawiającego. 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.