OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest **Dostawa i zakup sprzętu i licencji w ramach projektu pn. „Cyberbezpieczny Powiat Wołowski”.**
2. Wymagania ogólne dla dostarczanego sprzętu i oprogramowania (dotyczy wszystkich systemów opisanych w tym dokumencie):
    1) Opisane parametry techniczne są wymaganiami minimalnymi i wykonawca może zaoferować urządzenia o parametrach lepszych niż wymagane,
    2) Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów z obszaru Unii Europejskiej,
    3) Zamawiający wymaga, by dostarczone urządzenia były sprawne, nowe oraz by nie były używane, ani nieeksponowane na wystawach oraz imprezach targowych, nieuszkodzone, bezpieczne, kompletne tj. posiadające wszelkie akcesoria, niezbędne do użytkowania;
    4) Sprzęt musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis);
    5) Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa);
    6) Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich;
    7) Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
    8) Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
    9) Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekaże adresy WWW, pod którymi można je pobrać.
    10) Wykonawca jest zobowiązany do dostarczenia towaru do Starostwa Powiatowego w Wołowie, pl. Piastowski 2, 56 -100 Wołów na własny koszt w uzgodnionym z Zamawiającym terminie oraz rozładowania go i ustawienia we wskazanym przez Zamawiającego miejscu.
    11) Dostawa odbędzie się w dni robocze w godzinach pracy urzędu.
    12) Wykonawca zobowiązuje się do usunięcia na własny koszt wszelkich szkód spowodowanych przez wykonawcę i powstałych w trakcie realizacji zamówienia.
    13) Wykonawca jest odpowiedzialny względem Zamawiającego za wady przedmiotu zamówienia zmniejszające jego wartość lub użyteczność i w przypadku poniesienia z tego powodu strat, Wykonawca zobowiązuje się do ich pokrycia.
    14) Wskazane w dokumentach znaki towarowe, nazwy własne, itp. – stanowią wyłącznie wzorzec jakościowy, funkcjonalny, techniczny i technologiczny dotyczący przedmiotu zamówienia. We wszystkich przypadkach, w których ze względu na specyfikację przedmiotu zamówienia wskazano pochodzenie, nazwy materiałów, urządzeń, lub ich pochodzenie, dopuszcza się stosowanie materiałów, urządzeń równoważnych, tj. wszelkie wymienione z nazwy materiały, urządzenia użyte w przekazanej przez Zamawiającego dokumentacji lub ich pochodzenie, służą wyłącznie określeniu standardu i mogą być zastąpione innymi o nie gorszych parametrach technicznych, użytkowych, jakościowych, funkcjonalnych i walorach estetycznych, przy uwzględnieniu prawidłowej współpracy z pozostałymi materiałami, urządzeniami. Użyte w dokumentacji zamówienia nazwy, które wskazują

lub mogłyby kojarzyć się z producentem lub firmą, nie mają na celu preferowanie rozwiązań danego producenta lecz wskazanie na rozwiązanie, które powinno posiadać cechy techniczne, technologiczne nie gorsze od podanych w dokumentacji technicznej. Zamawiający w przypadku ofert zawierających rozwiązania równoważne będzie je weryfikować pod względem spełniania wymogów poszczególnych pozycji wymagań technicznych zawartych w załącznikach do Specyfikacji. Wykonawca zobowiązany jest udowodnić w ofercie równoważność oferowanych urządzeń lub systemów. Ciężar udowodnienia równoważności jest obowiązkiem Wykonawcy. Zamawiający nie uzna rozwiązań równoważnych, jeśli będą o gorszych niż wskazane w załącznikach do Specyfikacji minimalnych wymaganiach jakościowych, funkcjonalnych, technicznych i technologicznych.

15) Zamieszczone w dokumentacji zamówienia wymienione nazwy producentów (jeśli takie się pojawią) użyto jedynie w celu przykładowym. Ewentualnie wskazane nazwy produktów oraz ich producentów nie mają na celu naruszenie zasady uczciwej konkurencji i równego traktowania wykonawców. Wszędzie gdzie są one wskazane, należy czytać w ten sposób, że towarzyszy im określenie „lub równoważne". Przez pojęcie „lub równoważne" Zamawiający rozumie oferowanie materiałów gwarantujących realizację zadania zapewniających uzyskanie parametrów technicznych nie gorszych od założonych w wyżej wymienionych dokumentach. Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości przedmiotu zamówienia w stosunku do przewidzianych w dokumentacji technicznej, ani do zmiany ceny, ani do naruszenia przepisów prawa.
16) Odbiór sprzętu będącego przedmiotem umowy przez Zamawiającego nastąpi na podstawie protokołu odbioru (ilościowego i jakościowego).
17) Po dostarczeniu sprzętu przez Wykonawcę do miejsca wskazanego przez Zamawiającego, Zamawiający dokona odbioru ilościowego sprzętu, zaś w terminie do 5 dni roboczych liczonych od dnia dostawy dokona jego odbioru jakościowego (zwanego również odbiorem końcowym) potwierdzonego stosownym protokołem (tzn. protokół odbioru końcowego, upoważniający do wystawienia przez Wykonawcę faktury).
18) W przypadku stwierdzenia przez Zamawiającego, że Wykonawca dostarczył sprzęt niezgodny z opisem przedmiotu zamówienia i parametrach wynikających z oferty lub, że sprzęt jest niekompletny, lub posiada ślady zewnętrznego uszkodzenia, Zamawiający wezwie Wykonawcę do dostarczenia w terminie 5 dni roboczych od podpisania protokołu odbioru końcowego „z zastrzeżeniami" sprzętu zgodnego z opisem przedmiotu zamówienia, kompletnego i wolnego od wad. Procedura odbioru w takim przypadku wymagać będzie powtórzenia.
19) Zamawiający oraz Wykonawca wskażą osobę/osoby upoważnione do dokonania odbioru sprzętu.
20) W przypadku obiektywnej niemożliwości dostarczenia przez Wykonawcę sprzętu wskazanego w ofercie z powodu braku jego dostępności na rynku, co zostanie potwierdzone przez jego producenta, dopuszczalne jest dostarczenie przez Wykonawcę sprzętu o parametrach technicznych nie gorszych i cenie nie wyższej niż wynikające z oferty. W takim przypadku Wykonawca obowiązany jest uprzednio każdorazowo przedłożyć Zamawiającemu stosowne dokumenty (oświadczenie producenta o niedostępności zaoferowanego sprzętu, opinia o nie gorszych parametrach technicznych sprzętu zamiennego niż zaoferowany w ofercie). Zamiana zaoferowanego sprzętu wymaga zgody Zamawiającego, którą Zamawiający udzieli niezwłocznie, gdy otrzyma wymagane dokumenty.

1. Zarządzalny przełącznik sieciowy SAN

Parametr	Charakterystyka (wymagania minimalne)
Wymagania szczegółowe	Przełącznik FC musi być wykonany w technologii FC minimum 32 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, 4 Gb/s w zależności od rodzaju zastosowanych wkładek SFP. W przypadku obsadzenia portu FC za pomocą wkładki SFP 32Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 32, 16 lub 8 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji. W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji. Przełącznik FC musi być wyposażony, w co najmniej 8 aktywnych portów FC obsadzonych wkładkami SFP 32Gb/s z możliwością rozbudowy do 24 portów za pomocą odpowiedniej licencji i dodatkowych wkładek optycznych. Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 16Gb/s lub 32Gb/s w zależności od zastosowanych wkładek FC Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji (24 porty) wyposażonej we wkładki 32Gb/s musi wynosić minimum 768 Gb/s end-to-end. Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 900ns Rodzaj obsługiwanych portów, co najmniej: E, D oraz F. Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 24 aktywne porty 32Gbps to 80W Maksymalna ilość ciepła wydzielanego przez przełącznik FC wyposażony w 24 aktywne porty 32Gbps to 250 BTU na godzinę. Przełącznik FC musi być wyposażony w mechanizm agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu ISL Trunk o przepustowości minimum 256 Gb/s half duplex (dla wkładek 32Gbps) dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek. Przełącznik FC musi wspierać mechanizm balansowania ruchu, pomiędzy co najmniej 16 różnymi ścieżkami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o 3 parametry nagłówka ramki FC: DID, SID i OXID.

	Przełącznik FC musi zapewniać jednoczesną obsługę mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID. Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN. Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa: – mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric, – uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP, – uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP, – szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2, – definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control), – definiowane kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+, – szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS, – obsługa SNMP v1 oraz v3, – IP Filter dla portu administracyjnego przełącznika, – wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP, – wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP. Przełącznik FC musi mieć możliwość konfiguracji przez: – polecenia tekstowe w interfejsie znakowym konsoli terminala, – przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie. Przełącznik FC musi być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC: – logowanie zdarzeń poprzez mechanizm „syslog”, – ciągłe monitorowanie parametrów pracy przełącznika, portów, wkładek SFP i sieci fabric z automatycznym powiadamianiem administratora, wyłączeniem pracy portu lub przesunięciem przepływów tzw. slow drain na niski priorytet w przypadku przekroczenia zdefiniowanych wartości granicznych. Powiadamianie administrator musi być możliwe za pomocą wysyłania wiadomości e-mail, pułapki SNMP lub komunikatu w logu, – port diagnostyczny tzw. D_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami, testowe obciążenie połączenia pełną przepustowością 16Gbps/32Gbps oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością co najmniej do 5m dla wkładek SFP 16Gbps lub 32Gbps. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric, – FCping, – FC traceroute, – kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika,

	– Przełącznik musi być wyposażony w mechanizm sprzętowego monitorowania przepływów danych dla wskazanych jak i automatycznie wykrywanych par urządzeń komunikujących się przez dany port przełącznika. Dla każdego monitorowanego przepływu muszą być gromadzone statystyki dotyczące, co najmniej liczby wysłanych i odebranych ramek, przepustowości, liczby zapisów i odczytów SCSI, przy czym musi istnieć możliwość zawężenia zakresu monitorowania do następujących typów ramek: SCSI Reserve, SCSI Aborts, SCSI Read, SCSI Write, rejected frames, – Przełącznik musi być wyposażony w mechanizm sprzętowego generatora ruchu umożliwiającego symulowanie komunikacji w wielodomenowych sieciach SAN bez konieczności angażowania fizycznych urządzeń takich jak serwery lub macierze dyskowe, – Przełącznik musi być wyposażony w mechanizm umożliwiający kopiowanie pierwszych 64 bajtów ramek dla wybranych przepływów danych do pamięci lokalnej przełącznika w celu dalszej analizy, – Przełącznik musi być wyposażony w mechanizm umożliwiający sprzętowe identyfikowanie ramek FC oznaczonych parametrem VM ID oraz integrację tego mechanizmu z systemami monitorowania przepływów danych w szczególności w zakresie przepustowości oraz liczby zapisów i odczytów na sekundę. Po zainstalowaniu dodatkowej licencji przełącznik FC musi zapewnić możliwość przydzielenia, co najmniej 1700 tzw. buffer credits do pojedynczego portu FC przełącznika. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC. Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S. Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu. Przełącznik FC musi realizować kategoryzację ruchu na podstawie wartości parametru CS_CTL w nagłówku ramki FC oraz odpowiednie przydzielenie ramki do kategorii o wysokim, średnim lub niskim priorytecie. Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
Ilość	1 sztuka

2. Zakup macierzy dyskowej

Parametr	**Charakterystyka (wymagania minimalne)**

Obudowa	System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''. Maksymalna wysokość systemu nie może przekraczać 2U.
Dyski Twarde	Obsługa dysków twardych: System musi wspierać dyski: – SSD: od 800GB do 15.3TB, – SAS 10k od 900GB do 1800GB, – NL-SAS od 4TB do 18TB. System musi mieć możliwość rozbudowy do minimum 180 dysków oraz musi pozwalać na rozbudowę do wyższych modeli bez potrzeby migracji danych (przez rozbudowę do wyższego modelu zamawiający rozumie do modelu macierzy z większą ilością Cache, większą skalowalnością i mocniejszymi procesorami). Zamawiający dopuszcza rozwiązanie, które nie pozwala na taką rozbudowę w przypadku, gdy zostanie zaoferowany najwyższy z modeli macierzy skalowalny min do 500 dysków oraz pamięcią cache min 512GB. Macierz musi pozwalać i być przystosowana na rozbudowę do modelu NVME bez potrzeby wymiany dysków i kopiowania danych.
Kontroler	– Dwa kontrolery wyposażone w przynajmniej 8GB cache każdy, – W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash, – Macierz musi pozwalać na rozbudowę cache do 32GB cache na kontroler.
Interfejsy	Interfejsy: – Min. 4 porty 16 Gbps FC, – Min. 4 porty SAS 12 Gb/s do podłączenia półek dyskowych
RAID	– Wsparcie dla RAID: 0, 1, 5, 6, 10, – Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum 180 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych, – Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy.
Obsługiwane protokoły	– FC, – iSCSI, – SAS, – S3, – CIFS, – NFS. Zamawiający dopuszcza zrealizowanie protokołu CIFS, NFS i S3 za pomocą zewnętrznego oprogramowania typu Software Defined Storage.

Inne wymagania	Inne wymagania: – Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów: Microsoft® Windows Server®, Red Hat Enterprise Linux®, SUSE Linux Enterprise Server, VMware® ESX®, – Macierz musi posiadać funkcjonalność wykonywania snapshotów - minimum 128 per wolumen, – Macierz musi posiadać funkcjonalność klonowania danych, – Macierz musi posiadać funkcjonalność replikacji danych po FC (po zainstalowaniu portów FC na macierzy) w trybie synchronicznym i asynchronicznym, oraz po Ethernecie w trybie asynchronicznym system musi pozwalać na wykonanie do 32 jednoczesnych replikacji, – Macierz musi posiadać możliwość tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowa (ang. ThinProvisioning), – 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 dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 128 partycji, – Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online volumenów logicznych pomiędzy nimi w zależności od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika, – Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID, – Z poziomu graficznego interfejsu do zarządzania musi istnieć możliwość sprawdzenia stanu zużycia dysków SSD, – Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków, – Wraz z system musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście: wydajności i opóźnień na wolumenach, wydajności I/Ops, MB/s, – Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji, – Macierz musi posiadać oprogramowanie do aplikacji pozwalające na integrację z: Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter, VMware VASA, Microsoft Virtual Disk Service (VDS), Microsoft Virtual Shadow Service (VSS), – Zamawiający dopuszcza zaoferowanie zewnętrznego oprogramowania do zapewnienia integracji i monitoring w/w aplikacji np. w formie Software Defined storage, – Macierz musi pozwalać na szyfrowania danych, realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami.
Gwarancja i serwis	Inne wymagania: – Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów: Microsoft® Windows Server®, Red Hat Enterprise Linux®, SUSE Linux Enterprise Server, VMware® ESX®, – Macierz musi posiadać funkcjonalność wykonywania snapshotów - minimum 128 per wolumen, – Macierz musi posiadać funkcjonalność klonowania danych,

	– Macierz musi posiadać funkcjonalność replikacji danych po FC (po zainstalowaniu portów FC na macierzy) w trybie synchronicznym i asynchronicznym, oraz po Ethernecie w trybie asynchronicznym system musi pozwalać na wykonanie do 32 jednoczesnych replikacji, – Macierz musi posiadać możliwość tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowa (ang. ThinProvisioning), – 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 dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 128 partycji, – Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online volumenów logicznych pomiędzy nimi w zależności od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika, – Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID, – Z poziomu graficznego interfejsu do zarządzania musi istnieć możliwość sprawdzenia stanu zużycia dysków SSD, – Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków, – Wraz z system musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście: wydajności i opóźnień na wolumenach, wydajności I/Ops, MB/s, – Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji, – Macierz musi posiadać oprogramowanie do aplikacji pozwalające na integrację z: Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter, VMware VASA, Microsoft Virtual Disk Service (VDS), Microsoft Virtual Shadow Service (VSS), – Zamawiający dopuszcza zaoferowanie zewnętrznego oprogramowania do zapewnienia integracji i monitoring w/w aplikacji np. w formie Software Defined storage, – Macierz musi pozwalać na szyfrowania danych, realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami.
ilość	1 sztuka

3. Zakup systemu pamięci masowej

Parametr	**Charakterystyka (wymagania minimalne)**

Wymagania szczegółowe	W ramach postępowania należy dostarczyć minimum 8 dysków o pojemności min. 1.8TB o prędkości obrotowej 10000. Dyski muszą być zgodnie z macierzą dostarczaną w ramach niniejszego postępowania.
Ilość	1 komplet (komplet zawiera 8 dysków)

3. Zakup wsparcia do systemu pamięci masowej z wymiennymi modułami SFP

Parametr	**Charakterystyka (wymagania minimalne)**
Wymagania szczegółowe	W ramach postępowania należy dostarczyć wkładki współpracujące z oferowaną macierzą pozwalające na połączenia z hostami/przełącznikiem za pomocą protokołu FC o prędkości min. 16Gbps. – 4 szt.
Ilość	1 komplet (komplet składa się z 4 szt.)

5. Zakup przełączników sieciowych

Parametr	**Charakterystyka (wymagania minimalne)**
Wymagania szczegółowe	Zamawiający w ramach postępowania wymaga dostarczenia **2 urządzeń o** parametrach minimum : Urządzenie warstwy 3 w pełni zarządzane. Urządzenie wyposażone w minimum 48 portów 1 Gigabit Ethernet RJ45. Urządzenie musi posiadać lub mieć możliwość instalacji 4 portów 10 Gigabit Ethernet SFP+. Urządzenie muszą umożliwiać łączenie w stos składający się minimalnie z 4 urządzeń. Urządzenie musi zapewniać przepustowość nie mniejszą niż 176 Gbps. Szybkość przełączania urządzenia musi wynosić minimum 112 Mpps. Obsługa minimum: – 32 000 adresów MAC, – 2 000 tras IPv4, – 1 000 tras IPv6,

	Obsługa protokołu NTP. Obsługa IGMPv1/2/3. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: – IEEE 802.1w Rapid Spanning Tree, – Rapid Per-VLAN Spanning Tree (RPVST+), – IEEE 802.1s Multi-Instance Spanning Tree. Obsługa protokołu IEEE 802.1ab LLDP. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci: – Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+, – Obsługa list kontroli dostępu (ACL). Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci: – Możliwość obsługi kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), – Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, – Kontrola sztormów dla ruchu broadcast/multicast/unicast. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p. Urządzenie musi zapewniać możliwość routingu statycznego i dynamicznego dla IPv4 i IPv6. Urządzenie musi zapewniać wsparcie dla zaawansowanych protokołów routingu IPv4 (OSPF) i IPv6 (OSPFv3), routingu multicast (PIM-SM). Urządzenie musi zapewniać możliwość tworzenia statystyk ruchu w oparciu o sFlow lub równoważne. Obsługa protokołów SNMPv3, SSHv2, TFTP, HTTPS, SYSLOG. Maksymalny pobór mocy nie może przekraczać 50W. Możliwość montażu w szafie rack 19”. Wysokość Urządzenia nie może przekraczać 1 RU. Dostarczone Urządzenia muszą posiadać wszystkie potrzebne do ich prawidłowej pracy licencje co najmniej na cały okres trwania Umowy. Wraz z każdym urządzeniem należy dostarczyć 4 moduły 10Gbe SFP+ SR
Ilość	1 Komplet (komplet zawiera dwa urządzenia)

6. Zakup wsparcia oraz aktualizacji UTM

Parametr	Charakterystyka (wymagania minimalne)
Wymagania szczegółowe	Wymagania Ogólne System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: – Firewall, – Ochrony w warstwie aplikacji, – Protokołów routingu dynamicznego. Redundancja, monitoring i wykrywanie awarii – W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji, – Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych, – Monitoring stanu realizowanych połączeń VPN, – System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. Interfejsy, Dysk, Zasilanie: – System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 18 portami Gigabit Ethernet RJ-45, 8 gniazdami SFP 1 Gbps, 2 gniazdami SFP+ 10 Gbps, – System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. – System jest wyposażony w zasilanie 2xAC. Parametry wydajnościowe: – W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę, – Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B, – Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps,

	– Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps. – Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps. – Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps, – Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps. Funkcje Systemu Bezpieczeństwa: W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: – Kontrola dostępu - zapora ogniowa klasy Stateful Inspection, – Kontrola Aplikacji, – Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN, – Ochrona przed malware, – Ochrona przed atakami - Intrusion Prevention System, – Kontrola stron WWW, – Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, – Zarządzanie pasmem (QoS, Traffic shaping), – Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP), – Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site, – Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. – Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system, – Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). Polityki, Firewall – Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń, – System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: – Translację jeden do jeden oraz jeden do wielu, – Dedykowany ALG (Application Level Gateway) dla protokołu SIP, – W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN, – Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, – Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe, – Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna,

	– Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu: Amazon Web Services (AWS), Microsoft Azure, Cisco ACI, Google Cloud Platform (GCP), OpenStack,, VMware NSX, Kubernetes. Połączenia VPN System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: – Wsparcie dla IKE v1 oraz v2, – Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM), – Obsługa protokołu Diffie-Hellman grup 19, 20, – Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, – Tworzenie połączeń typu Site-to-Site oraz Client-to-Site, – Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności, – Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego, – Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat, – Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu, – Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu, – Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth, – Mechanizm „Split tunneling” dla połączeń Client-to-Site. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: – Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0., – Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta, – Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. Routing i obsługa łączy WAN W zakresie routingu rozwiązanie zapewnia obsługę: – Routingu statycznego, – Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM, – Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu, – ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu, – BFD (Bidirectional Forwarding Detection),

	– Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. Funkcje SD-WAN – System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN, – SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). Zarządzanie pasmem – System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu, – System daje możliwość określania pasma dla poszczególnych aplikacji, – System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP, – System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. Ochrona przed malware – Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021), – Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS, – System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości, – System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów, – System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android), – Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora, – System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze, – System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików, – Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta, – Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu, – Możliwość rozbudowania Systemu o dodatkową funkcjonalność wstrzymania dostarczenia pliku, dla którego jest realizowana analiza z wykorzystaniem systemu Sandbox, do czasu otrzymania werdyktu z systemu Sandbox. Ochrona przed atakami – Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych, – System chroni przed atakami na aplikacje pracujące na niestandardowych portach,

	– Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora, – Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur, – System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS, – Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty), – Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http, – Wykrywanie i blokowanie komunikacji C&C do sieci botnet, – Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie, – Możliwość rozbudowania Systemu o sygnatury do ochrony przed atakami na systemy przemysłowe SCADA. Kontrola aplikacji – Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP, – Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora, – Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików, – Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P, – Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. – Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021), – System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). Kontrola WWW – Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne, – W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy, – Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard, – Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL, – Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). – Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony, – Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo, – Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW,

	– System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. Uwierzytelnianie użytkowników w ramach sesji – System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu, Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych, – System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego, – System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie, – Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. Zarządzanie – Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania, – Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów, – Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego, – System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow, – System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację, – Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall, – Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone, – Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM), – Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. Logowanie – Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej, – W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania,

	– Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa, – Możliwość włączenia logowania per reguła w polityce firewall, – System zapewnia możliwość logowania do serwera SYSLOG, – Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS, – Możliwość rozbudowania Systemu o dodatkowe usługi: logowania, raportowania, korelacji zdarzeń realizowanych w chmurze. Testy wydajnościowe oraz funkcjonalne – Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy. Serwisy i licencje Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są **licencje**: – Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen **od dnia dostarczenia sprzętu co najmniej do dnia 17.06.2026 r.** Gwarancja oraz wsparcie – Gwarancja: System jest objęty serwisem gwarancyjnym producenta, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. – Serwis urządzeń musi byś realizowany przez producenta lub autoryzowanego partnera serwisowego producenta – **wymagane oświadczenie Wykonawcy potwierdzające, że serwis będzie realizowany przez Producenta lub autoryzowanego partnera serwisowego producenta (należy dołączyć do oferty),** – Serwis urządzeń musi być realizowany zgodnie z wymaganiami normy ISO 9001 **– do oferty należy dołączyć dokument potwierdzający, że serwis urządzeń będzie realizowany zgodnie z tą normą,** – Firma serwisująca musi posiadać **certyfikat nadany przez uprawniony podmiot potwierdzający realizację usług zgodnie z normą ISO 27001 lub certyfikat równoważny (należy załączyć do oferty).**
Ilość	1 sztuka

7. Zakup zasilaczy UPS

Nazwa	Minimalne wymagania dla sprzętu
Moc pozorna	Min 850 VA

Moc czynna	Min 480 W
Architektura UPS-a	line-interactive
Liczba faz na wejściu	1 (230V)
Liczba akumulatorów	Min 1
Napięcie	12 V
Pojemność akumulatora	Min 9 Ah
Czas przełączenia	Maks. 10 ms
Czas transferu	Maks 6ms
Czas ładowania	6 h
Typ obudowy	Tower
Zabezpieczenia / filtry	Przeciwprzepięciowe
Funkcje specjalne	Automatyczna regulacja napięcia (AVR)
Porty zasilania we.	Wtyczka sieciowa
Porty zasilania wy.	Min 2 x gniazda francuskie
Gniazda we/wy	Min 1 x USB (Type B) Min 2 x RJ-11/RJ-45
Pozostałe parametry	- Obsługiwane systemy operacyjne Win. 98, Win. 2000, Win. XP, Win. Vista, Win. 7, Linux, FreeBSD, Win. Millenium, Win. 8, Win. Vista 64bit, Win. 7 64bit, Win. 8 64bit, Windows 10, Windows 10 64bit
Gwarancja	Min 24 miesiące
Ilość	40 sztuk

8. Zakup serwera wraz z instalacją i konfiguracją

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	– Obudowa Rack o wysokości max 1U z możliwością instalacji 8 dysków 2.5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli, – Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.
Płyta główna	– Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym, – Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci.
Chipset	– Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych.
Procesor	– Jeden procesor 4-rdzeniowy, min. 3.4GHz, umożliwiający osiągnięcie wyniku min. 50.8 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org w konfiguracji jednoprocesorowej.

Pamięć RAM	– 1x32GB pamięci RAM DDR5 UDIMM o częstotliwości pracy 4800MT/s.
Karta Graficzna	– Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200.
Wbudowane porty	– min. 4 porty USB w tym 1 port USB 3.0 z tyłu obudowy, – 1 port VGA na tylnym panelu, – 1 port RS232.
Interfejsy sieciowe/FC/SAS	– Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie Base-T.
Kontroler RAID	– Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10.
Dyski twarde	– Zainstalowane: 2x dysk SAS 10k o pojemności min. 1.2TB, Hot-Plug, – Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Zasilacze	– Redundantne, o mocy maks. 700W klasy Titanium.
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, – 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 posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: – zdalny dostęp do graficznego interfejsu Web karty zarządzającej, – zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera), – szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika, – możliwość podmontowania zdalnych wirtualnych napędów, – wirtualną konsolę z dostępem do myszy, klawiatury, – wsparcie dla IPv6, – wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish, – możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer,

	– możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer, – integracja z Active Directory, – możliwość obsługi przez dwóch administratorów jednocześnie, – wsparcie dla dynamic DNS, – wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej, – możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera, – możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności 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).
Certyfikaty	– Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001, – Serwer musi posiadać deklaracja CE, – Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. – 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 przez wykonawcę usługi wsparcia technicznego z zakresu wdrażanej technologii, – Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 9/5 następującymi kanałami: telefonicznie, przez Internet, – Serwis urządzeń musi byś realizowany przez producenta lub autoryzowanego partnera serwisowego producenta – **wymagane oświadczenie Wykonawcy potwierdzające, że serwis będzie realizowany przez Producenta lub autoryzowanego partnera serwisowego producenta (należy dołączyć do oferty),**

	– Serwis urządzeń musi być realizowany zgodnie z wymaganiami normy ISO 9001 – **do oferty należy dołączyć dokument potwierdzający, że serwis urządzeń będzie realizowany zgodnie z tą normą,** – Firma serwisująca musi posiadać **certyfikat nadany przez uprawniony podmiot potwierdzający realizację usług zgodnie z normą ISO 27001 lub certyfikat równoważny (należy załączyć do oferty).**
System operacyjny	System operacyjny: Oprogramowanie Microsoft Windows Serwer Standard 2022 lub równoważne spełniające poniższe warunki zgodności: – Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji, – Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, – Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, – Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, – Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, – Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, – Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy, – Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading, – Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, – Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji, – Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. – Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, – Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, – Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, – Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji, – Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), – Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, – Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), – Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,

	– Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
Oprogramowanie backup	Wymagania ogólne: – Oprogramowanie musi umożliwiać objęcie kopią zapasową 20 maszyn wirtualnych, oraz dostarczone musi być z licencją i wsparciem technicznym. Zamawiający wymaga **czasu licencji ważnej co najmniej do dnia 17.06.2026 r.,** – 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, – 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, – 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, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. Całkowite koszty posiadania: – Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej, – Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków, – Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji, – Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu, – Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli, – Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier, – Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu, – Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania,

	– Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time), – Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu, – Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API, – Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji, – Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji, – Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania – Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych, – Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej, – Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np. skasowanie backupu, dodanie kolejnego administratora), – Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS), – Oprogramowanie musi posiadać integracje z systemami typu SIEM, – Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji. Wymagania RPO: – Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej, – Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych, – Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru, – Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku Vmware, – Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją Vmware, – Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592), – Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) – Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard,

	– Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS, – Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN, – Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji, – Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO, – Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik – Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding), – Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN). Wymagania RTO: – Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych, – Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna), – Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami, – Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej 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, – 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 wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego, – Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur, – Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji, – Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux, – Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux, – Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji, – Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN, – Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle, – Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI, – Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2, – Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN. Ograniczenie ryzyka: – Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna), – Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach, – Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu

	testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem, – Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32, – Oprogramowanie musi 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 umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. Środowiska fizyczne: – Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego, – Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych, – Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, – Rozwiązanie musi wspierać system operacyjny macOS, – Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix, – Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą), – Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster, – Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów, – Rozwiązanie musi wspierać backup podłączonych dysków USB, – Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym, – Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury), – Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone , – Rozwiązanie musi wspierać kontrolę pasma sieciowego, – Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych, – Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN,

	– Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft, – Rozwiązanie musi wspierać technologię BitLocker, – Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania, – Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych – Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych, – Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu, – Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform, – Rozwiązanie musi wspierać szyfrowanie, – Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne, – Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego, – Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej, – Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.
ilość	1 sztuka

9. Zakup licencji FortiGate 100E dla zapewnienia bezpieczeństwa sieciowego dla infrastruktury IT

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	W ramach postępowania Zamawiający wymaga dostarczenia licencji dla posiadanego obecnie urządzenia klasy UTM Fortigate 100E o numerze seryjnym: FG100E4Q16004950. **Koniec obecnej licencji nastąpi 17.07.2025 r.,** Zamawiający wymaga dostarczenia **czasu licencji ważnej od 18.07.2025 r. co najmniej do dnia 17.06.2026 r.**
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagana jest licencja zapewniająca: Kontrolę Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analizę typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Gwarancja i wsparcie	System ma zostać objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
ilość	1 sztuka

10. Zakup licencji do oprogramowania antywirusowego

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	W ramach postępowania Zamawiający wymaga dostarczenia licencji dla posiadanego obecnie oprogramowania antywirusowego FortiClient EMS EPP/APT dla 125 endpointów o numerze seryjnym: FCTEMS8821005057. Koniec obecnej licencji nastąpi 17.07.2025 r. , **Zamawiający wymaga dostarczenia czasu licencji ważnej od dnia 18.07.2025 r. co najmniej do dnia 17.06.2026 r.**
Serwisy i licencje	Licencje powinny obejmować: Endpoint Protection Platform (EPP), Advanced Threat Protection (ATP), VPN, ZTNA (Zero Trust Network Access) oraz zarządzanie urządzeniami końcowymi za pomocą lokalnego serwera EMS.
Gwarancja i wsparcie	System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
ilość	1 sztuka

11. Zakup licencji do oprogramowania do tworzenia kopii zapasowych

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	Wymagania ogólne: – 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,

	– 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 **Koniec obecnej licencji 25.01.2025 r., Zamawiający wymaga dostarczenia licencji ważnej od dn. 26.01.2025 r. co najmniej 12 miesięcy.** – 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, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux, – Oprogramowanie musi umożliwiać backup dla 20 maszyn wirtualnych i posiadać wsparcie techniczne na okres równy okresowi udzielonej gwarancji. Całkowite koszty posiadania: – Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej, – Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków, – Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji, – Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu, – Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli, – Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier, – Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu, – Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania, – Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time), – Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu, – Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API, – Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji,

	– Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji, – Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania – Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych, – Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej, – Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np. skasowanie backupu, dodanie kolejnego administratora), – Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS), – Oprogramowanie musi posiadać integracje z systemami typu SIEM, – Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji. Wymagania RPO: – Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej, – Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych, – Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru, – Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku Vmware, – Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją Vmware, – Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592), – Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) – Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard, – Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS, – Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN, – Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami

	ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji, – Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO, – Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik – Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding), – Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN). Wymaganie RTO: – Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych, – Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna), – Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami, – Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej 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, – 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 wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego, – Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur, – Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji, – Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux, – Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux, – Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji, – Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN, – Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle, – Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI, – Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2, – Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN, Ograniczenie ryzyka: – Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna), – Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach, – Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem, – Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32,

	– Oprogramowanie musi 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 umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego, Środowiska fizyczne: – Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego, – Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych, – Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, – Rozwiązanie musi wspierać system operacyjny macOS, – Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix, – Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą), – Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster, – Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów, – Rozwiązanie musi wspierać backup podłączonych dysków USB, – Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym, – Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury), – Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone, – Rozwiązanie musi wspierać kontrolę pasma sieciowego, – Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych, – Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN – Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft, – Rozwiązanie musi wspierać technologię BitLocker, – Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania,

	– Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych – Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych, – Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu, – Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform, – Rozwiązanie musi wspierać szyfrowanie, – Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne, – Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego, – Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej, – Rozwiązanie musi wspierać tworzenie wielu zadań backupowych, Monitoring: – System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich – System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 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 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, – System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter, – System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn, – System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel, – System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk – System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora, – System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów, – System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard), – System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna,

	– System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego, – System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta, – System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych, – System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu, – System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware, – System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4. Raportowanie: – System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie, – System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 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, – System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów, – System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V, – System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF, – System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc, – System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach, – System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów, – System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych, – System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych, – System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury, – System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta, – System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych,

	– System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’, – System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware, – System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots), – System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.
ilość	1 sztuka