

Opis przedmiotu zamówienia

Część 1:

1. Macierz dyskowa

Zamawiana ilość: 1 sztuka

Parametr	Charakterystyka (wymagania minimalne)
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19", o wysokości maksymalnie 2U z możliwością instalacji min. 24 dysków 2.5"
Przestrzeń dyskowa	Zainstalowane: 24 x dysk SAS min. 12 Gb/s min. 10K 2,5" o pojemności min. 2.4TB, Hot-Plug
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych.
Obsługa dysków	Macierz musi mieć możliwość obsługi dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5" jak również 3,5".
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności

Parametr	Charakterystyka (wymagania minimalne)
	<p>macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).</p> <p>Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.</p>
Tryb pracy kontrolerów macierzowych	<p>Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.</p>
Pamięć cache	<p>Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM.</p> <p>Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.</p> <p>Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania baterijnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.</p>
Rozbudowa pamięci cache	<p>Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.</p> <p>Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.</p>
Interfejsy	<p>Macierz musi posiadać, co najmniej 8 portów 25Gb iSCSI (4 porty na kontroler)</p>
Kable/wkładki	<p>2x kabel DAC 10GbE SFP+ min. 2m.</p>
Zarządzanie	<p>Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.</p>

Parametr	Charakterystyka (wymagania minimalne)
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	<p>Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej.</p> <p>Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>
Thin Provisioning	<p>Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.</p> <p>Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>
Tiering	<p>Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS.</p> <p>Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.</p> <p>Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.</p>
Wewnętrzne kopie migawkowe	<p>Macierz musi umożliwiać dokonywanie na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii.</p> <p>Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.</p>

Parametr	Charakterystyka (wymagania minimalne)
	Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).

Parametr	Charakterystyka (wymagania minimalne)
	<p>Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix.</p> <p>Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.</p>
Redundancja	<p>Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.</p> <p>Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.</p> <p>Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.</p> <p>Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.</p>
Dodatkowe wymagania	<p>Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.</p>

Parametr	Charakterystyka (wymagania minimalne)
	Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International). Wymagane dołączenie do oferty oświadczenia Producenta lub Wykonawcy potwierdzające spełnienie powyższych zaleceń.
Inne	<p>Urządzenie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta.</p> <p>Urządzenie musi być wyprodukowane zgodnie z normami ISO 9001 oraz ISO 14001 – do oferty należy załączyć certyfikaty ISO 9001 oraz ISO 14001 dla producenta oferowanej macierzy.</p> <p>Urządzenie musi posiadać deklarację zgodności CE – do oferty należy załączyć deklarację zgodności CE dla oferowanej macierzy.</p>
Warunki gwarancji	<p>Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres min. 5 lat.</p> <p>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.</p> <p>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.</p> <p>Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</p> <p>Technik Producenta lub firmy serwisującej z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.</p> <p>Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</p> <p>Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek</p>

Parametr	Charakterystyka (wymagania minimalne)
	<p>sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.</p> <p>W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Do oferty należy załączyć oświadczenie podmiotu realizującego serwis lub oświadczenie producenta sprzętu lub oświadczenie Wykonawcy potwierdzające, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk pozostanie u Zamawiającego.</p> <p>Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:</p> <ul style="list-style-type: none"> • Możliwości utworzenia zgłoszenia serwisowego, w wyniku którego proces diagnostyki odbędzie się na miejscu w siedzibie Zamawiającego. • Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. • Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. • Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.

Parametr	Charakterystyka (wymagania minimalne)
	<ul style="list-style-type: none"> • Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Zamawiającego w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. <p>Serwis może być realizowany wyłącznie przez producenta sprzętu i / lub we współpracy z autoryzowanym partnerem serwisowym producenta.</p> <p>Do oferty należy załączyć oświadczenia producenta lub Wykonawcy potwierdzające, że serwis sprzętu będzie realizowany bezpośrednio przez producenta i / lub we współpracy z autoryzowanym partnerem serwisowym producenta.</p>

2. UPS

Zamawiana ilość: 1 sztuka

Parametr	Charakterystyka (wymagania minimalne)
Typ urządzenia	Zasilacz awaryjny UPS centralny
Technologia	True On-Line Double Conversion
Moc znamionowa	≥ 20 kVA / 20 kW
Współczynnik mocy wyjściowej	1,0
Konfiguracja faz	3-fazowe wejście / 3-fazowe wyjście (3:3)
Napięcie wejściowe nominalne	Min. 380 / 400 / 415 VAC
Zakres napięcia wejściowego	min. 304–485 VAC przy 100% obciążenia
Zakres częstotliwości wejściowej	40–70 Hz
THDi (zniekształcenia prądu wejściowego)	$\leq 3\%$
Wejściowy współczynnik mocy	$\geq 0,99$
Napięcie wyjściowe nominalne	Min. 380 / 400 / 415 VAC
Regulacja napięcia wyjściowego	$\pm 1\%$ (statyczna), $\pm 2\%$ (dynamiczna)
Częstotliwość wyjściowa	50 / 60 Hz $\pm 0,05$ Hz
Odporność na przeciążenia	min. 105% przez ≥ 60 min
Sprawność w trybie on-line	$\geq 96\%$
Sprawność w trybie ECO	$\geq 99\%$
Współczynnik szczytu	3:1
Typ akumulatorów	VRLA / AGM / GEL
Start z baterii	Tak

Parametr	Charakterystyka (wymagania minimalne)
Konfigurowalna liczba baterii	Tak
Czas ładowania baterii	do 90% pojemności w czasie ≤ 8 godzin
Czas podtrzymania	Przy obciążeniu 100% minimum 5 minut
Układ ładowania	Inteligentny, z kompensacją temperaturową
Bypass automatyczny	Tak
Bypass serwisowy	Tak
Złącze EPO	Tak
Interfejsy komunikacyjne	min. USB, RS232, RS485, RJ45
Styki bezpotencjałowe	min. 6 wejść/wyjść typu Dry Contact
Możliwość integracji z NMS/BMS	Tak (SNMP lub równoważne)
Panel sterowania	Kolorowy, dotykowy wyświetlacz LCD
Praca równoległa	Obsługa konfiguracji redundantnych i pojemnościowych
Poziom hałasu	≤ 58 dB przy 100% obciążenia
Stopień ochrony obudowy	IP20
Zakres temperatur pracy	$0^{\circ}\text{C} \div +40^{\circ}\text{C}$
Normy bezpieczeństwa	CE
Instalacja	<p>W ramach zamówienia Wykonawca zapewni podłączenie, konfigurację oraz uruchomienie zasilacza awaryjnego UPS wraz z przekazaniem do eksploatacji Zamawiającemu.</p> <p>Zakres usługi obejmuje co najmniej:</p> <ul style="list-style-type: none"> • posadowienie urządzenia w miejscu wskazanym przez Zamawiającego, • podłączenie UPS do instalacji elektrycznej (wejście, wyjście, tor bypassu), • podłączenie i konfigurację układu baterijnego, • weryfikację poprawności połączeń elektrycznych i komunikacyjnych,

Parametr	Charakterystyka (wymagania minimalne)
	<ul style="list-style-type: none"> • konfigurację podstawowych parametrów pracy UPS, • uruchomienie urządzenia w trybie pracy produkcyjnej, • przeprowadzenie testów poprawności działania (w tym testów bypassu i pracy bateryjnej), • przekazanie urządzenia do użytkowania Zamawiającemu, • krótkie instruktażowe omówienie zasad obsługi dla personelu Zamawiającego. <p>Usługa musi zostać wykonana przez personel posiadający odpowiednie kwalifikacje i doświadczenie w instalacji oraz uruchamianiu zasilaczy UPS klasy enterprise.</p>
Warunki gwarancji	Producenta min. 24 miesiące

3. Urządzenie do składowania danych kopii bezpieczeństwa

Zamawiana ilość: 1 sztuka

Parametr	Charakterystyka (wymagania minimalne)
Dedykowane urządzenie do backupu	Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli.
Pojemność warstwy aktywnej / Skalowalność netto	Dostarczone urządzenie musi oferować przestrzeń min. 16TB bez uwzględniania mechanizmów protekcji – przestrzeń dedykowana do gromadzenia deduplikatów, wymagana skalowalność do min. 170TB (powierzchni użytkowej widocznej po założeniu systemu plików).
Warstwa chmurowa	Dostarczone urządzenie powinno umożliwiać rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityką retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemieszczane (w postaci zdedykowanej) na dodatkową warstwę, wymagane wsparcie dla AWS, Microsoft Azure oraz Google GCP. Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń min. 80TB dla warstwy CLOUD.
Interfejsy sieciowe i obsługa protokołów	Oferowane urządzenie musi posiadać minimum 4 porty 10/25Gb/s Eth OP (wymagana pełna obsada wkładek). Wymagana możliwość obsługi każdym z w/w portów protokołów CIFS, NFS, deduplikacja na źródle.
Wieloprotokołowość	Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami: <ul style="list-style-type: none"> • CIFS, NFS; • zapewniającym deduplikację na źródle, wymagane wsparcie dla aplikacji Commvault (co najmniej na poziomie Media Server a także Client Direct przy użyciu storage accelerator), Veeam

Parametr	Charakterystyka (wymagania minimalne)
	<p>Backup and Replication (co najmniej na poziomie Veeam Data Mover), NetWorker na poziomie standardowego klienta</p> <ul style="list-style-type: none"> VTL (min. 10 jednocześnie).
Licencjonowanie pakietowe (All-in-One)	<p>Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, deduplikacja na źródle, VTL do oferowanej pojemności urządzenia.</p>
Zagregowana przepustowość	<p>Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: NFS co najmniej 25 TB/h (dane podawane przez producenta) oraz co najmniej 50 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta).</p>
Limit jednoczesnych strumieni danych	<p>Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie:</p> <ul style="list-style-type: none"> zapis danych minimum 150 strumieniami; odczyt danych minimum 50 strumieniami; replikacja minimum 50 strumieniami; <p>pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.</p> <p>Wymienione wartości 250 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu i jednocześnie 50 strumieni dla odczytu i jednocześnie 50 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.</p> <p>Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.</p>
Emulacja bibliotek taśmowych VTL	<p>Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych:</p> <ul style="list-style-type: none"> StorageTek L180

Parametr	Charakterystyka (wymagania minimalne)
	<ul style="list-style-type: none"> IBM TS 3500
Emulacja napędów taśmowych	Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7.
Skalowalność zasobów VTL (napędy/sloty)	Urządzenie musi umożliwiać (w przypadku VTL'a) emulację minimum 250 napędów, emulację min. 30 000 slotów w przypadku poj. biblioteki taśmowej oraz emulację sumarycznie min. 60 000 slotów.
Deduplikacja w locie (In-line)	Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.
Przetwarzanie bloków o zmiennej długości	Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o wielkości nie większej niż 12 kB. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych, co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości.
Globalna deduplikacja międzyprotokołowa	Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na

Parametr	Charakterystyka (wymagania minimalne)
	<p>urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany.</p> <p>Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A”, nie może zostać ponownie zapisany, jeśli trafi do innej wirtualnej biblioteki „B” w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych.</p>
Silnik deduplikacji w pamięci RAM	<p>Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. Wymaganie nie będzie spełnione, jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backup’ową. Wymaganie deduplikacji in-line dotyczy zapisu danych przez każdy z wymaganych interfejsów, w przypadku interfejsów: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie może w żadnym stopniu zależeć od konkretnej aplikacji backup’owej, dane zapisywane poprzez interfejsy NFS CIFS bez użycia jakiegokolwiek aplikacji backup’owej również muszą być deduplikowane w sposób in-line</p>
Bezpośredni zapis danych zdeduplikowanych na dysk	<p>Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line).</p>
Kompresja lokalna (algorytm LZ)	<p>Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.</p>

Parametr	Charakterystyka (wymagania minimalne)
System plików o strukturze dziennika (Log-structured)	Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane, dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymaganie dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem / modyfikacją danych.
Ekosystem wsparcia bibliotek DD Boost	<p>Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Commvault, Veeam Backup and Replication, NetWorker.</p> <p>W przypadku współpracy z każdą z poniższych aplikacji:</p> <ul style="list-style-type: none"> • Commvault • Veeam Backup and Replication • NetWorker <p>urządzenie musi umożliwiać deduplikację na źródle (w przypadku Commvault: co najmniej na poziomie Media Server a także Client Direct przy użyciu storage accelerator, w przypadku Veeam Backup and Replication co najmniej na poziomie Veeam Data Mover), w przypadku NetWorker na poziomie standardowego klienta) i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.</p> <p>Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby do oferowanego urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu.</p>
Deduplikacja na źródle przez Fibre Channel (DFO)	W przypadku przyjmowania backupów z Commvault, Veeam Backup and Replication, NetWorker, urządzenie musi umożliwiać deduplikację na źródle (co najmniej na poziomie Media Server dla CommVault, Data Mover dla Veeam, klienta dla NetWorker) i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC.

Parametr	Charakterystyka (wymagania minimalne)
	Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby do oferowanego urządzenia były transmitowane poprzez sieć FC jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu.
Natychmiastowe odtwarzanie maszyn wirtualnych	Oferowane urządzenie musi umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych.
Grupy interfejsów DD Boost (ifgroups)	Wymagana funkcjonalność Load Balancing oraz Link Failover w obrębie portów (Eth) wykorzystywanych przez aplikację backupową.
Wirtualne pełne kopie syntetyczne (DD Boost)	Wymagane wsparcie dla backupów typu Virtual Synthetics w przypadku aplikacji Commvault, Veeam Backup and Replication oraz NetWorker.
Szyfrowanie danych w transmisji	W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
Szyfrowanie danych spoczywających (At-rest)	Urządzenie powinno umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia.
Obsługa klientów DD Boost over FC	Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych: <ul style="list-style-type: none"> • Windows • Linux (RedHat, SuSE)
Topologie replikacji danych	Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów: <ul style="list-style-type: none"> • jeden do jednego • wiele do jednego • jeden do wielu • kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C).

Parametr	Charakterystyka (wymagania minimalne)
	Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację jest również przedmiotem zamówienia.
Izolacja sieci replikacyjnej	Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.
Wielofunkcyjna konfiguracja interfejsów	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
Replikacja zarządzana z poziomu aplikacji (MFR)	<p>W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana możliwość kontroli przez: Commvault oraz NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:</p> <ul style="list-style-type: none"> • replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących, • replikacji podlegają tylko te fragmenty danych (na poziomie bloków używanych do deduplikacji), które nie znajdują się na docelowym urządzeniu, • replikacja zarządzana jest z poziomu wymaganej aplikacji, • aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji.
Próg operacyjny zajętości systemu plików	Oferowane urządzenie musi działać poprawnie przy wypełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ewentualne problemy, obostrzenia, które są efektem wypełnienia urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.

Parametr	Charakterystyka (wymagania minimalne)
Dławienie (throttling) pasma replikacji	Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji.
Ochrona RAID 6 (podwójna parzystość)	Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej.
Zarządzanie migawkami (Snapshots)	Oferowane urządzenie musi pozwalać na realizację oraz przechowywanie SnapShot'ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot'u. Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtworzenia backupów).
Skalowalność liczby migawek	Urządzenie musi pozwalać na przechowywanie minimum 500 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.
Logiczne kontenery danych (MTree)	Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia).
Skalowalność struktury MTree	Urządzenie musi mieć możliwość podziału na minimum 10 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 10 logicznych części pracujących równolegle z pełną wydajnością urządzenia.
Uprawnienia i kwoty (quotas) dla MTree	Dla każdej z wyżej wskazanych logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby

Parametr	Charakterystyka (wymagania minimalne)
	logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia.
Wielonajemność (Multi-tenancy)	<p>Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia jako niezależnego urządzenia dostępnego za pośrednictwem:</p> <ul style="list-style-type: none"> • CIFS • NFS • VTL • deduplikacja na źródle
Blokada retencji (Retention Lock Compliance / Governance)	<p>Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku. Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):</p> <ol style="list-style-type: none"> 1. Możliwość zdjęcia blokady przed upływem ważności danych. 2. Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE), w tym wypadku wymagane wsparcie norm SEC 17a-4(f) oraz ISO Standard 15489-1 w zakresie ochrony danych, wymagane oficjalne wsparcie wymaganej blokady przez aplikację Commvault, Veeam Backup and Replication oraz NetWorker. <p>Licencje na blokadę usunięcia / zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem.</p> <p>Wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady. W każdym przypadku wymagana również możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności SnapShot.</p>
Blokowanie plików na udziałach NFS/CIFS	Urządzenie musi mieć możliwość przechowywania danych niezmiennych:

Parametr	Charakterystyka (wymagania minimalne)
	<ul style="list-style-type: none"> • Video • Grafika • Nagrania dźwiękowe • Pliki pdf na udziałach CIFS/NFS.
Architektura DIA (Data Invulnerability Architecture)	Urządzenie musi weryfikować dane po zapisie (nie chodzi o ewentualną weryfikację danych indeksowych generowanych przez urządzenie, ale o weryfikację wszystkich zabezpieczanych danych backup'owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja musi być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność.
Proces czyszczenia (Garbage Collection)	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.
Działanie procesu czyszczenia w tle	Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).
Dławienie intensywności procesu czyszczenia	Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora).
Harmonogram zadań konserwacyjnych	Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równoległe z procesami backup/restore/replication.

Parametr	Charakterystyka (wymagania minimalne)
Optymalna częstotliwość cyklu czyszczenia	Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas, w którym backupy / odtworzenia narażone są na spowolnienie.
Próg automatycznego uruchomienia czyszczenia	Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni.
Interfejsy zarządzania (Graficzny i Linii Komend)	Urządzenie musi mieć możliwość zarządzania poprzez: <ul style="list-style-type: none"> • Interfejs graficzny dostępny z przeglądarki internetowej. • Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell).
Zintegrowane oprogramowanie zarządzające	Oprogramowanie do zarządzania musi rezydować na oferowanym urządzeniu deduplikacyjnym.
Pre-weryfikacja aktualizacji systemu (Ewaluator)	Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade'ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem.
Zintegrowana architektura sprzętowo-programowa	Urządzenie musi być rozwiązaniem kompletnym, apłiancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway.
Warunki gwarancji	Oferowane urządzenie powinno być objęte min. 3 letnim wsparciem producenta działającym w trybie Next Business Day. Uszkodzone nośniki pozostają u Zamawiającego bez ponoszenia dodatkowych kosztów.
Inne	Urządzenie musi posiadać deklarację zgodności CE – do oferty należy załączyć deklarację zgodności CE dla oferowanego urządzenia.

4. Oprogramowanie do gromadzenia i analizy logów

Zamawiana ilość: 1 sztuka

Parametr	Charakterystyka (wymagania minimalne)
Przeznaczenie	Oprogramowanie do centralnego zbierania, przetwarzania, analizy oraz raportowania logów zdarzeń z infrastruktury IT.
Centralne gromadzenie logów	Możliwość agregacji logów w jednym repozytorium z wielu źródeł jednocześnie.
Liczba obsługiwanych źródeł logów	Obsługa co najmniej 150 źródeł logów jednocześnie.
Obsługiwane źródła logów	Wsparcie dla pozyskiwania logów co najmniej z: serwerów, urządzeń sieciowych, zapór / UTM klasy enterprise (w tym Stormshield lub równoważnych), zasilaczy UPS oraz innych urządzeń IT wspierających standardowe mechanizmy logowania.
Metody zbierania logów	Obsługa min.: Syslog (UDP/TCP), zbieranie agentowe i bezagentowe, import strumieni lub plików logów.
Normalizacja i parsowanie	Mechanizmy parsowania, normalizacji i kategoryzacji logów (typ zdarzenia, źródło, poziom krytyczności, użytkownik, adres IP).
Przetwarzanie i obróbka danych	Filtrowanie, agregacja, wyszukiwanie pełnotekstowe oraz analiza zdarzeń w zadanych zakresach czasu.
Korelacja zdarzeń	Możliwość korelowania zdarzeń pochodzących z różnych źródeł (czas, urządzenie, użytkownik, adres IP, typ zdarzenia).
Raportowanie	Raporty predefiniowane i definiowane przez użytkownika; harmonogramowanie raportów; eksport min. do PDF i CSV.
Alerty i powiadomienia	Konfigurowalne reguły alertów; powiadomienia w czasie rzeczywistym lub cykliczne; wysyłka alertów min. pocztą elektroniczną.
Dashboard / wizualizacja	Webowy panel zarządzania z konfigurowalnymi dashboardami prezentującymi zdarzenia, trendy i statystyki.
Retencja danych	Możliwość przechowywania logów przez okres co najmniej 12 miesięcy.
Zarządzanie retencją	Konfigurowalne polityki retencji, archiwizacji i usuwania danych.

Parametr	Charakterystyka (wymagania minimalne)
Uprawnienia i audyt	Role użytkowników i uprawnienia; rejestrowanie działań administracyjnych (logi audytowe).
Integracja	Możliwość integracji z innymi systemami (np. poprzez API, eksport danych lub przekazywanie alertów).
Wydajność i skalowalność	Obsługa 150 źródeł logów bez degradacji funkcjonalności; możliwość rozbudowy systemu w przyszłości.
Dostęp	Dostęp administracyjny i użytkowy przez przeglądarkę internetową.
Licencjonowanie	Licencja wieczysta. Zamawiający dopuszcza rozwiązanie oparte na licencji open source.
Dokumentacja	Dokumentacja wdrożeniowa i administracyjna w języku polskim lub angielskim.
Wdrożenie	Wdrożenie obejmuje: <ul style="list-style-type: none"> • instalację i konfigurację systemu analizy logów, • połączenie min. 10 źródeł logów, w tym serwerów, urządzeń sieciowych, zapory/UTM oraz UPS, • konfigurację reguł parsowania i normalizacji logów, • uruchomienie raportów oraz dashboardów, • konfigurację alertów dla zdarzeń krytycznych, • testy poprawności zbierania, przetwarzania i prezentacji logów, • przekazanie systemu do eksploatacji Zamawiającemu, • instruktaż administracyjny dla personelu Zamawiającego.

5. Oprogramowanie do wykonywania kopii bezpieczeństwa

Zamawiana ilość: 20 sztuk

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	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

Parametr	Charakterystyka (wymagania minimalne)
	<p>na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.</p> <p>Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i / lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. Licencja wieczysta dla 20 serwerów (fizyczne i VM).</p>
Wymagania szczegółowe	<p>Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.</p> <p>Oprogramowanie musi tworzyć „samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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,</p>

Parametr	Charakterystyka (wymagania minimalne)
	<p>oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.</p> <p>Oprogramowanie musi wspierać niezmiennosc kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.</p> <p>Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.</p> <p>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).</p> <p>Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.</p> <p>Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.</p> <p>Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.</p> <p>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.</p> <p>Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.</p> <p>Oprogramowanie musi posiadać architekturę klient / serwer z możliwością instalacji wielu instancji konsoli administracyjnych.</p>

Parametr	Charakterystyka (wymagania minimalne)
	Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.
Wymagania RPO	<p>Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.</p> <p>Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.</p> <p>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.</p> <p>Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów.</p> <p>Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.</p> <p>Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.</p> <p>Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.</p> <p>Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).</p> <p>Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla</p>

Parametr	Charakterystyka (wymagania minimalne)
	<p>Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.</p> <p>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.</p> <p>Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.</p> <p>Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V.</p> <p>Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.</p> <p>Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.</p> <p>Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.</p> <p>Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).</p> <p>Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).</p>
Wymagania RTO	<p>Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania,</p>

Parametr	Charakterystyka (wymagania minimalne)
	<p>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.</p> <p>Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).</p> <p>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.</p> <p>Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.</p> <p>Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.</p> <p>Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.</p> <p>Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.</p> <p>Oprogramowanie musi umożliwić odtworzenie plików / folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez</p>

Parametr	Charakterystyka (wymagania minimalne)
	<p>potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.</p> <p>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.</p> <p>Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell.</p> <p>Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.</p> <p>Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.</p> <p>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.</p> <p>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.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe</p>

Parametr	Charakterystyka (wymagania minimalne)
	<p>bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.</p> <p>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.</p> <p>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.</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle.</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI.</p> <p>Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.</p>
Wymagania ograniczenia ryzyka	<p>Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).</p> <p>Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.</p> <p>Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według</p>

Parametr	Charakterystyka (wymagania minimalne)
	<p>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.</p> <p>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.</p> <p>Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.</p>
Wymagania dla Agenta	<p>Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.</p> <p>Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych.</p> <p>Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE.</p> <p>Rozwiązanie musi wspierać system operacyjny macOS.</p> <p>Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix.</p> <p>Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą).</p> <p>Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster.</p>

Parametr	Charakterystyka (wymagania minimalne)
	<p>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.</p> <p>Rozwiązanie musi wspierać backup podłączonych dysków USB.</p> <p>Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym.</p> <p>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).</p> <p>Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle.</p> <p>Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone.</p> <p>Rozwiązanie musi wspierać kontrolę pasma sieciowego.</p> <p>Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych.</p> <p>Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN.</p> <p>Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft.</p> <p>Rozwiązanie musi wspierać technologię BitLocker.</p> <p>Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania.</p> <p>Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1</p>

Parametr	Charakterystyka (wymagania minimalne)
	<p>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.</p> <p>Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych.</p> <p>Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.</p> <p>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.</p> <p>Rozwiązanie musi wspierać szyfrowanie.</p> <p>Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache), gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne.</p> <p>Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego.</p> <p>Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej.</p> <p>Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.</p>

6. UTM

Zamawiana ilość: 2 sztuki

Parametr	Charakterystyka (wymagania minimalne)
Obsługa sieci	Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
Zapora korporacyjna (firewall)	<ol style="list-style-type: none"> 1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówek pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI, tj. na podstawie adresów mac. 7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.

Parametr	Charakterystyka (wymagania minimalne)
	<p>9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.</p> <p>10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).</p> <p>11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.</p>
Intrusion Prevention System (IPS)	<p>1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.</p> <p>2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.</p> <p>3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.</p> <p>4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.</p> <p>5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.</p> <p>6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.</p> <p>7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.</p>

Parametr	Charakterystyka (wymagania minimalne)
	<ol style="list-style-type: none"> Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. Moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
Kształtowanie pasma (Traffic Shapping)	<ol style="list-style-type: none"> Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
Ochrona antywirusowa	<ol style="list-style-type: none"> Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się, aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również, żeby analiza sandboxingu była przeprowadzana przez firmy trzecie (inne niż producent rozwiązania). Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania).

Parametr	Charakterystyka (wymagania minimalne)
	<ol style="list-style-type: none"> Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź, gdy analiza skanerem antywirusowym została zakończona błędem. Skaner antywirusowy ma pochodzić od europejskiego producenta. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku, jaki będzie poddawany analizie skanerem antywirusowym. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
Ochrona antyspam	<ol style="list-style-type: none"> Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). Ochrona antyspam ma działać w oparciu o: <ol style="list-style-type: none"> Białe / czarne listy, DNS RBL, Skaner heurystyczny. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
Wirtualne sieci prywatne (VPN)	<ol style="list-style-type: none"> Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). Urządzenie ma wspierać co najmniej następujące typy sieci VPN: <ol style="list-style-type: none"> PPTP VPN, IPSec VPN, SSL VPN. SSL VPN ma działać w trybie tunelu. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.

Parametr	Charakterystyka (wymagania minimalne)
	<ol style="list-style-type: none"> Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal). Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
Filtr dostępu do stron www	<ol style="list-style-type: none"> Urządzenie ma posiadać wbudowany filtr URL. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu. Administrator ma mieć możliwość dodawania własnych kategorii URL. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: <ol style="list-style-type: none"> blokowanie dostępu do adresu URL, zezwolenie na dostęp do adresu URL, blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.

Parametr	Charakterystyka (wymagania minimalne)
	<ol style="list-style-type: none"> 7. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 8. Filtr URL musi uwzględniać komunikację po protokole HTTPS. 9. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 10. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. 11. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.
Uwierzytelnianie	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: <ol style="list-style-type: none"> a) lokalną bazę użytkowników (wewnętrzny LDAP), b) zewnętrzną bazę użytkowników (zewnętrzny LDAP), c) usługę katalogową Microsoft Active Directory. 2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. 3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: <ol style="list-style-type: none"> a) SSL, b) Radius, c) Kerberos. 4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

Parametr	Charakterystyka (wymagania minimalne)
	<p>7. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).</p> <p>8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).</p> <p>9. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.</p> <p>10. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.</p>
Administracja łączami do Internetu (ISP)	<p>1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).</p> <p>2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:</p> <ul style="list-style-type: none"> a) równoważenie względem adresu źródłowego, b) równoważenie względem połączenia. <p>3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.</p> <p>4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).</p> <p>5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.</p>

Parametr	Charakterystyka (wymagania minimalne)
	<ol style="list-style-type: none"> 6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów). 7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
Routing (trasowanie)	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 5. Rozwiązanie musi dawać możliwość wybrania predefiniowanego obiektu typu blackhole.
Administracja urządzeniem	<ol style="list-style-type: none"> 1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 6. Urządzenie ma umożliwiać zarządzania z poziomu konsoli (SSH).

Parametr	Charakterystyka (wymagania minimalne)
	<ol style="list-style-type: none"> 7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. 10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. 12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). 13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). 14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. 15. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku. 16. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).

Parametr	Charakterystyka (wymagania minimalne)
	<p>17. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.</p> <p>18. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:</p> <ul style="list-style-type: none"> a) manualnego eksportu do pliku w dowolnym momencie czasu, b) automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu <p>19. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.</p> <p>20. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.</p> <p>21. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.</p>
Raportowanie	<p>1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.</p> <p>2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.</p> <p>3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.</p> <p>4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.</p> <p>5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.</p>

Parametr	Charakterystyka (wymagania minimalne)
	<ol style="list-style-type: none"> 6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
Pozostałe usługi i funkcje	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. 2. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 3. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 4. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 5. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). 6. Urządzenie ma posiadać usługę DNS Proxy. 7. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). 8. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. 9. Urządzenie musi mieć zaimplementowane Open API. 10. Urządzenie ma posiadać dwie niezależne partycje, np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe

Parametr	Charakterystyka (wymagania minimalne)
	<p>zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.</p> <p>11. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN.</p> <p>Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.</p>
Parametry sprzętowe	<ol style="list-style-type: none"> 1. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB. 2. Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy. 3. Liczba portów Ethernet 2,5Gbps – min. 8. 4. Liczba portów światłowodowych 10Gbps – min. 6. 5. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 6. Urządzenie ma być wyposażone w min. 2, różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45. 7. Przepustowość Firewall (1518 bajtów UDP) – minimum 38Gbps. 8. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 10Gbps. 9. Przepustowość filtrowania Antywirusowego – minimum 2Gbps. 10. Przepustowość tunelu VPN przy szyfrowaniu AES-GCM – minimum 4Gbps. 11. Liczba tuneli VPN IPSec – minimum 1 000. 12. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 300. 13. Obsługa interfejsów 802.11q (VLAN) – minimum 1336. 14. Liczba równoczesnych sesji – minimum 1 000 000 i nie mniej niż 50 000 nowych sesji / sekundę.

Parametr	Charakterystyka (wymagania minimalne)
	<p>15. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.</p> <p>16. Urządzenie musi być wyposażone w moduł TPM.</p> <p>17. Urządzenie nie ma limitu na liczbę użytkowników.</p> <p>18. Liczba reguł filtrowania – minimum 32 768.</p> <p>19. Liczba tras statycznego routingu – minimum 5 120.</p> <p>20. Liczba tras dynamicznego routingu – minimum 10 000.</p> <p>21. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U.</p>
Logi	<p>Wymagania ogólne:</p> <ol style="list-style-type: none"> 1. W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa. 2. Rozwiązanie musi zostać dostarczone w postaci maszyny wirtualnej instalowanej w środowisku Vmware lub Windows Hyper-V. 3. Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW. 4. Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów. 5. Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP. 6. Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta. 7. Rozwiązanie musi posiadać predefiniowane panele dla informacji z urządzeń pracujących w sieci OT. <p>Zarządzanie Logami:</p> <ol style="list-style-type: none"> 1. Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.

Parametr	Charakterystyka (wymagania minimalne)
	<ol style="list-style-type: none"> 2. Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS. 3. Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder). 4. Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta. <p>Rodzaje wyszukiwania:</p> <ol style="list-style-type: none"> 1. Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie. 2. Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.). 3. Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne. 4. Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP). 5. Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów). 6. Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV. <p>Raportowanie:</p> <ol style="list-style-type: none"> 1. Rozwiązanie musi umożliwiać tworzenie statycznych raportów. 2. Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób. 3. Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów. 4. Rozwiązanie musi umożliwiać tworzenie własnych raportów.

Parametr	Charakterystyka (wymagania minimalne)
	<p>5. Rozwiązanie musi umożliwiać tworzenie dynamicznych raportów (w czasie rzeczywistym) z funkcjonalnością „drill-down”.</p> <p>Zarządzanie incydentami:</p> <ol style="list-style-type: none"> 1. Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email. 2. Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie. <p>Wymagania systemowe:</p> <ol style="list-style-type: none"> 1. Liczba zdarzeń na sekundę (EPS): min. 10 000. 2. Zarządzanie logami: min. 1 rok. 3. Liczba obsługiwanych urządzeń: min. 500. 4. Liczba zapisu zdarzeń na dobę: min 13000 MB.
Warunki gwarancji	<p>Urządzenie ma być objęte min. 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.</p> <p>W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.</p>

7. Serwer NAS

Zamawiana ilość: 1 sztuka

Parametr	Charakterystyka (wymagania minimalne)
Procesor	Procesor osiągający wynik minimum 4300 punktów w teście PassMark.
Obudowa	Typu rack o wysokości maksymalnie 4U wraz z szynami przesuwными w zestawie.
Pamięć RAM	Minimum 32GB DDR4– pamięć RAM tego samego producenta co serwer NAS.
Ilość obsługiwanych dysków	Minimum 16 dysków 3,5" /2,5" SATA 6 Gb/s o maksymalnej pojemności nie mniejszej niż 20TB każdy.
Interfejsy sieciowe	Minimum 2 porty 2.5GbE RJ-45, Minimum 4 porty 10GSFP+. Obsługa agregacji łączy, VLAN i Jumbo Frame.
Porty i złącza	Minimum 1 port USB 3.2 Gen 2 typu A (10 Gb/s)
Gniazda PCIe	Minimum 2 gniazda PCIe Gen3 x4.
Wskaźniki LED	Stan serwera, LAN, USB, HDD 1–16
Obsługa RAID	RAID 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity, RAID 5, 6, 10 + dysk zapasowy.
Funkcje RAID	Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD.
Szyfrowanie	256-bitowe szyfrowanie AES folderów oraz szyfrowanie dysków zewnętrznych.
Wsparcie dla systemów operacyjnych	Apple Mac OS 10.10 lub nowszy Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux IBM AIX 7, Solaris 10 lub nowszy UNIX Microsoft Windows 7, 8, 10, 11 Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP

Parametr	Charakterystyka (wymagania minimalne)
Usługi	Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer WWW, Serwer plików, Manager plików przez WWW, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
Język GUI	Polski
Typowy pobór mocy podczas pracy	Maksymalnie 200 W
System plików	Dyski wewnętrzne - ZFS. Dyski zewnętrzne - EXT3, EXT4, NTFS, FAT32, HFS+.
Liczba kont użytkowników	Minimum 4096
Liczba grup	Minimum 512
Liczba udziałów	Minimum 256
Zasilanie	Redundantny zasilacz o mocy minimum 500W.
Warunki gwarancji	Minimum 60 miesięcy gwarancji producenta.

8. Dysk twardy do NAS

Zamawiana ilość: 30 sztuk

Parametr	Charakterystyka (wymagania minimalne)
Opis	<p>Pojemność: min. 20 TB</p> <p>Format: 3.5 "</p> <p>Interfejs: SATA min. 6Gb/s</p> <p>Prędkość obrotowa: min. 7200 rpm</p> <p>Bufor: min. 256 MB</p> <p>MTBF: min. 2.000.000 h</p> <p>Informacje dodatkowe: min. 5 lat gwarancji.</p> <p>Dysk przeznaczony do serwerów NAS bez limitu zatok.</p> <p>Dysk kompatybilny z urządzeniem z punktu 7 oraz urządzeniem Qnap TS-1273AU-RP-8G.</p>

9. Instalacja, konfiguracja oraz wdrożenie zakupionego sprzętu i oprogramowania

Parametr	Charakterystyka (wymagania minimalne)
Opis	<p>Przedmiotem zamówienia jest wykonanie usługi instalacji, konfiguracji oraz wdrożenia dostarczonej infrastruktury IT i oprogramowania do Zamawiającego, obejmującej systemy pamięci masowej, urządzenia do składowania kopii zapasowych, serwer NAS, system backupu, zaporę sieciową UTM.</p> <p>1. Macierz dyskowa klasy enterprise</p> <p>Zakres prac obejmuje:</p> <ul style="list-style-type: none"> • montaż urządzenia w szafie RACK, • konfigurację grup RAID zgodnie z wymaganiami Zamawiającego, • konfigurację wolumenów logicznych i puli dyskowych, • podłączenie macierzy do serwerów, • testy poprawności działania, wydajności i redundancji, • przygotowanie do eksploatacji. <p>2. Urządzenie do składowania kopii zapasowych danych</p> <p>Zakres prac obejmuje:</p> <ul style="list-style-type: none"> • instalację urządzenia w szafie RACK, • konfigurację systemu operacyjnego i przestrzeni dyskowej (16 TB), • konfigurację interfejsów sieciowych 10 Gb/s SFP+, • integrację z infrastrukturą sieciową Zamawiającego, • przygotowanie urządzenia do współpracy z oprogramowaniem backupowym, • testy zapisu i odczytu danych. <p>3. Oprogramowanie do tworzenia kopii zapasowych</p> <p>Zakres prac obejmuje:</p> <ul style="list-style-type: none"> • instalację i aktywację licencji oprogramowania backupowego,

Parametr	Charakterystyka (wymagania minimalne)
	<ul style="list-style-type: none"> • konfigurację repozytoriów kopii zapasowych (macierz / urządzenie deduplikacyjne / NAS), • konfigurację zadań backupu i polityk retencji, (przeniesienie obecnych zadań i polityk), • konfigurację harmonogramów kopii zapasowych (przeniesienie obecnych harmonogramów), • testy wykonywania kopii oraz odtwarzania danych, • konfigurację podstawowych raportów i powiadomień. <p>4. Zapora sieciowa UTM</p> <p>Zakres prac obejmuje:</p> <ul style="list-style-type: none"> • instalację urządzenia w szafie RACK, • montaż i konfigurację modułów światłowodowych 10 Gb/s, • konfigurację interfejsów sieciowych i stref bezpieczeństwa, • konfigurację podstawowych polityk zapory (przeniesienie obecnych polityk), • konfigurację usług bezpieczeństwa (w tym ochrona UTM, sandbox), • konfigurację logowania zdarzeń i przekazywania logów do systemu analizy logów, • testy poprawności działania i bezpieczeństwa. <p>5. Serwer NAS</p> <p>Zakres prac obejmuje:</p> <ul style="list-style-type: none"> • instalację urządzenia w szafie RACK, • rozbudowę pamięci RAM oraz instalację kart sieciowych 10 Gb/s, • instalację i inicjalizację dysków 20 TB (w tym konfigurację puli produkcyjnych oraz dysków zapasowych), • konfigurację macierzy RAID i wolumenów, • konfigurację usług udostępniania danych, • testy dostępności i wydajności.

Parametr	Charakterystyka (wymagania minimalne)
	<p>6. Integracja i testy końcowe</p> <p>Zakres prac obejmuje:</p> <ul style="list-style-type: none"> • integrację wszystkich elementów infrastruktury (macierz, backup, NAS, UTM), • weryfikację poprawności komunikacji sieciowej, • testy scenariuszy awaryjnych (backup / restore, dostępność danych), • optymalizację konfiguracji pod kątem wydajności i bezpieczeństwa. <p>Wykonawca w trakcie realizacji czynności instalacji, konfiguracji i wdrożenia dostarczonego sprzętu i oprogramowania zobowiązany jest do bieżącego zgłaszania Zamawiającemu wprowadzanych zmian w systemach należących do Zamawiającego, a po zakończeniu czynności wdrożeniowych również do przekazania Zamawiającemu dokumentacji opisującej wprowadzone zmiany.</p>

Pozostałe wymagania:

Zamawiający wymaga, by:

- 1) dostarczony w ramach umowy sprzęt był kompletny i fabrycznie nowy, tj. nieużywany i nieregenerowany oraz by nie był nigdzie wcześniej montowany lub aktywowany. Sprzęt ten musi zostać dostarczony w oryginalnym, nienaruszonym opakowaniu, posiadającym zabezpieczenia zastosowane przez producenta.
- 2) dostarczone w ramach umowy oprogramowanie nie było nigdy wcześniej używane, rejestrowane i aktywowane.
- 3) dostarczone w ramach umowy oprogramowanie powinno zostać dostarczone Zamawiającemu w najnowszej, stabilnej wersji. Zamawiający dopuszcza również rozwiązanie pozwalające na zaktualizowanie dostarczonego Zamawiającemu oprogramowania do najnowszej, stabilnej wersji w trakcie procesu jego wdrożenia.

- 4) dostarczony w ramach umowy sprzęt i oprogramowanie nie może być obciążone prawami osób lub podmiotów trzecich, musi pochodzić z legalnego kanału sprzedaży producenta a także musi być wolny od wad fizycznych i prawnych.

Ogólne zasady równoważności rozwiązań:

- 1) W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych powyżej, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii, funkcjonalności i wydajności wyszczególnionych w rozwiązaniach wyspecyfikowanych powyżej, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności jak te wyspecyfikowane przez Zamawiającego w inny, niż podany sposób. Za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego przez Zamawiającego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana rozwiązania na równoważne nie zakłóciła bieżącej pracy Starostwa Powiatowego w Nowym Dworze Mazowieckim. W tym celu Wykonawca musi do rozwiązania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, uwzględnić niezbędną asystę pracowników

Wykonawcy w operacji uruchamiania rozwiązania równoważnego w środowisku produkcyjnym itp.

- 2) Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) sprzętu lub danego rozwiązania technologicznego Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych wobec tych wskazanych przez Zamawiającego pod warunkiem, że zapewnią uzyskanie parametrów technicznych nie gorszych niż wymagane przez Zamawiającego w niniejszej dokumentacji. Zamawiający informuje, że w takiej sytuacji przedmiotowe zapisy są jedynie przykładowe i stanowią wskazanie dla Wykonawcy, jakie cechy powinny posiadać składniki użyte do realizacji przedmiotu zamówienia. Zamawiający zgodnie z art. 99 ust. 6 ustawy z dnia 11 września 2019r. – Prawo zamówień publicznych (t.j. Dz.U. z 2024r. poz. 1320 z późn.zm.), zwanej dalej „ustawą Pzp”, dopuszcza oferowanie urządzeń lub rozwiązań równoważnych. Urządzenia lub rozwiązania pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, jakim muszą odpowiadać urządzenia lub rozwiązania oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami urządzeń lub rozwiązań ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów lub produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub konkretne rozwiązanie technologiczne przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu lub rozwiązania technologicznego, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach.
- 3) Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia, o których mowa w ustawie Pzp, dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez

Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia wraz z ofertą stosownych dokumentów, uwiarygodniających te rozwiązania.

Część 2:

1. Szkolenie z cyberbezpieczeństwa dla kadry zarządzającej

Parametr	Charakterystyka (wymagania minimalne)
Opis	<p>Zakres szkolenia:</p> <ol style="list-style-type: none"> Główne założenia i wymagania prawne dotyczące cyberbezpieczeństwa w pracy urzędnika: <ol style="list-style-type: none"> Czym jest cyberbezpieczeństwo; Od czego zależy bezpieczeństwo informacji; Obowiązki Jednostek samorządu terytorialnego wynikające z obowiązujących aktów prawnych związanych z bezpieczeństwem informacji. Przegląd najpopularniejszych zagrożeń oraz zasady bezpiecznego korzystania z Internetu: <ol style="list-style-type: none"> Czym są ataki socjotechniczne; Rodzaje ataków (phishing, spearphishing, vishing, smishing, quishing); Jak rozpoznać atak; Jakie dane chcą pozyskać przestępcy; Jak uniknąć zagrożenia; Przydatne narzędzia. Bezpieczeństwo fizyczne w ochronie informacji: <ol style="list-style-type: none"> Regulacje i zasady, które należy stosować w biurze; Fizyczne metody ochrony informacji; Ochrona nośników informacji; Bezpieczna praca poza biurem. Bezpieczeństwo haseł: <ol style="list-style-type: none"> Statystyki ataków na hasła;

Parametr	Charakterystyka (wymagania minimalne)
	<ul style="list-style-type: none"> b) Hasła w upublicznionych wyciekach; c) Zasady tworzenia silnych haseł; d) Metody ochrony haseł. <p>5. Bezpieczne korzystanie z witryn internetowych:</p> <ul style="list-style-type: none"> a) Na co zwrócić uwagę przed otwarciem witryny; b) Najnowsze przykłady fałszywych witryn; c) Jak się chronić. <p>6. Przegląd znanych typów ataków na samorządy:</p> <ul style="list-style-type: none"> a) Ransomware i inne rodzaje ataków najczęściej kierowane na JST; b) Skutki ataków dla JST; c) Jak się chronić przed atakami. <p>7. Moduł dla kadry zarządzającej:</p> <ul style="list-style-type: none"> a) System Zarządzania Bezpieczeństwem Informacji oparty o normę ISO 27001:2023 - wymagania i procedury. b) Zarządzanie ryzykiem w bezpieczeństwie informacji. c) Ciągłość działania – wymagania oparte na normie ISO 22301. d) Zarządzanie incydem w urzędzie. <p>Szkolenie na miejscu u Zamawiającego.</p> <p>Ilość osób do przeszkolenia: 15 osób.</p> <p>Ilość grup: min. 1.</p> <p>Ilość osób w grupie: max. 15 osób.</p> <p>Czas szkolenia 1 grupy: min. 4 h.</p> <p>Ukończenie szkolenia musi zostać potwierdzone imiennymi certyfikatami wydanymi uczestnikom.</p>

2. Platforma szkoleniowa

Parametr	Charakterystyka (wymagania minimalne)
Przedmiot zamówienia	<p>Przedmiotem zamówienia jest dostawa, wdrożenie oraz udostępnienie platformy szkoleniowej z zakresu cyberbezpieczeństwa dla pracowników Starostwa Powiatowego w Nowym Dworze Mazowieckim, przeznaczonej do podnoszenia świadomości zagrożeń cybernetycznych oraz kształtowania bezpiecznych nawyków w pracy z systemami informatycznymi. Platforma udostępniona Zamawiającemu powinna pozwolić na przeszkolenie 40 użytkowników.</p>
Wymagania funkcjonalne platformy	<p>Zakres szkoleniowy:</p> <p>Materiały szkoleniowe z zakresu cyberbezpieczeństwa obejmujące m.in.:</p> <ul style="list-style-type: none"> • bezpieczeństwo informacji, • phishing i socjotechnikę, • bezpieczną pracę z pocztą elektroniczną, • hasła i uwierzytelnianie wieloskładnikowe, • ochronę danych osobowych, • zagrożenia ransomware, • bezpieczną pracę z dokumentami, urządzeniami mobilnymi i nośnikami danych. <p>Aktualność treści:</p> <p>Regularna aktualizacja treści szkoleniowych zgodnie z aktualnymi zagrożeniami cybernetycznymi.</p> <p>Forma szkoleń:</p> <p>Kursy e-learningowe, materiały multimedialne, filmy instruktażowe, prezentacje, krótkie moduły edukacyjne oraz testy wiedzy.</p> <p>Indywidualizacja szkoleń:</p> <p>Możliwość przypisywania szkoleń do użytkowników, grup lub ról organizacyjnych.</p>

Parametr	Charakterystyka (wymagania minimalne)
	<p>Ścieżki szkoleniowe:</p> <p>Możliwość tworzenia i zarządzania ścieżkami szkoleniowymi dla różnych grup użytkowników.</p> <p>Testy i egzaminy:</p> <p>Wbudowane mechanizmy testów wiedzy, quizów oraz weryfikacji postępów szkoleniowych.</p> <p>Symulacje zagrożeń:</p> <p>Realizacja symulowanych kampanii socjotechnicznych (np. phishing) wraz z oceną reakcji użytkowników.</p> <p>Automatyczne przypomnienia:</p> <p>Automatyczne powiadomienia o rozpoczęciu, terminach i zaległościach szkoleniowych.</p> <p>Raportowanie:</p> <p>Rozbudowane raporty dotyczące frekwencji, wyników testów, skuteczności szkoleń i poziomu świadomości użytkowników.</p> <p>Dashboard administracyjny:</p> <p>Panel administracyjny prezentujący bieżący stan realizacji szkoleń i poziom ryzyka.</p> <p>Zarządzanie użytkownikami:</p> <p>Centralne zarządzanie kontami użytkowników, rolami i uprawnieniami.</p> <p>Integracja:</p> <p>Możliwość integracji z systemami tożsamości (np. import użytkowników) lub innymi systemami IT Zamawiającego.</p> <p>Dostępność:</p> <p>Dostęp do platformy przez przeglądarkę internetową z komputerów i urządzeń mobilnych.</p>

Parametr	Charakterystyka (wymagania minimalne)
	<p>Język:</p> <p>Interfejs użytkownika i treści szkoleniowe w języku polskim.</p> <p>Bezpieczeństwo danych:</p> <p>Przetwarzanie i przechowywanie danych użytkowników zgodnie z obowiązującymi przepisami.</p> <p>Licencjonowanie:</p> <p>Licencja umożliwiająca korzystanie z platformy przez okres co najmniej 12 miesięcy od dnia udostępnienia platformy użytkownikom po stronie Zamawiającego. Dostęp do Platformy zostanie udostępniony użytkownikom po stronie Zamawiającemu w dniu zakończenia czynności wdrożeniowych opisanych poniżej.</p> <p>Wsparcie techniczne:</p> <p>Dostęp do wsparcia technicznego oraz aktualizacji funkcjonalnych w okresie trwania licencji.</p> <p>Dokumentacja:</p> <p>Dokumentacja administracyjna i użytkowa w formie elektronicznej.</p> <p>Rozliczalność:</p> <p>Platforma powinna umożliwiać generowanie certyfikatów imiennych potwierdzających ukończenie szkolenia przez danego użytkownika.</p> <p>W przypadku braku takiej możliwości dopuszcza się również, by funkcja ta została zastąpiona przez możliwość generowania raportów potwierdzających listę użytkowników, którzy przeszli szkolenie zgodnie ze stanem na dany, wskazany przez Zamawiającego dzień.</p>
Wdrożenie platformy	<p>Zakres wdrożenia obejmuje:</p> <ul style="list-style-type: none"> • konfigurację środowiska platformy szkoleniowej, • konfigurację struktury organizacyjnej oraz ról użytkowników, • import lub utworzenie kont użytkowników (40 osób),

Parametr	Charakterystyka (wymagania minimalne)
	<ul style="list-style-type: none"> • konfigurację podstawowych polityk szkoleniowych i harmonogramów, • uruchomienie przykładowych szkoleń i testów wiedzy, • konfigurację raportów i powiadomień, • przeprowadzenie testów poprawności działania platformy, • przekazanie platformy do użytkowania Zamawiającemu. <p>Wdrożenie zostanie przeprowadzone przez Wykonawcę w terminie maksymalnie 3 dni roboczych od dnia zawarcia umowy powierzenia przetwarzania danych osobowych pomiędzy Zamawiającym a Wykonawcą.</p>
Wsparcie i utrzymanie	<ul style="list-style-type: none"> • zapewnienie wsparcia technicznego w okresie obowiązywania licencji, • aktualizacje treści szkoleniowych oraz mechanizmów platformy, • pomoc w rozwiązywaniu bieżących problemów eksploatacyjnych.

3. Szkolenia informatyczne

Parametr	Charakterystyka (wymagania minimalne)
Szkolenie typ 1	<p>Autoryzowane szkolenie producenta serwerowego systemu operacyjnego. Min. 40 godzin szkolenia obejmującego następujące zagadnienia:</p> <ol style="list-style-type: none"> 1. Wprowadzenie do administracji systemu operacyjnego Windows Server. 2. Usługi zarządzania tożsamością. 3. Usługi infrastruktury sieciowej. 4. Serwery plików i zarządzanie pamięcią masową. 5. Wirtualizacja Hyper-V i kontenery. 6. Wysoka dostępność. 7. Odzyskiwanie danych po awarii. 8. Bezpieczeństwo. 9. Usługi pulpitu zdalnego.

Parametr	Charakterystyka (wymagania minimalne)
	<p>10. Dostęp zdalny i usługi internetowe.</p> <p>11. Monitorowanie serwera i wydajności.</p> <p>12. Aktualizacja i migracja.</p> <p>Możliwość dostawy vouchera szkoleniowego z terminem ważności do dnia 15.09.2026r.</p> <p>Ukończenie szkolenia musi zostać potwierdzone imiennymi certyfikatami wydanymi uczestnikom.</p> <p>Ilość osób do przeszkolenia: 2.</p> <p>Forma szkolenia: stacjonarne (w siedzibie Zamawiającego) lub online.</p>
Szkolenie typ 2	<p>Szkolenie cyberbezpieczeństwa min. 40 godzin, obejmujące następujące zagadnienia:</p> <ol style="list-style-type: none"> 1. Wprowadzenie do etycznego hakingu (Introduction to Ethical Hacking). 2. Zbieranie informacji o ataku (Footprinting and Reconnaissance). 3. Skanowanie sieci (Scanning Networks). 4. Enumeracja (Enumeration). 5. Analiza podatności (Vulnerability Analysis). 6. Hackowanie systemu (System Hacking). 7. Złośliwe oprogramowanie (Malware Threats) Monitorowanie i przechwytywanie danych (Sniffing). 8. Inżynieria społeczna – socjotechniki (Social Engineering). 9. Ataki DDoS (Denial-of-Service). 10. Przejęcie / przechwytywanie sesji (Session Hijacking). 11. Omijanie IDS, zapór Firewall i Honeypots (Evading IDS, Firewalls, and Honeypots). 12. Hakowanie serwerów sieciowych (Hacking Web Servers). 13. Hakowanie aplikacji internetowych (Hacking Web Applications). 14. Ataki przez zapytania w SQL (SQL Injection).

Parametr	Charakterystyka (wymagania minimalne)
	<p>15. Hakowanie sieci bezprzewodowych (Hacking Wireless Networks).</p> <p>16. Hakowanie mobilnych platform (Hacking Mobile Platforms).</p> <p>17. Hakowanie Internetu Rzeczy (IoT Hacking).</p> <p>18. Bezpieczeństwo chmury (Cloud Computing).</p> <p>19. Kryptografia (Cryptography).</p> <p>Możliwość dostawy vouchera szkoleniowego z terminem ważności do dnia 15.09.2026r.</p> <p>Ukończenie szkolenia musi zostać potwierdzone imiennymi certyfikatami wydanymi uczestnikom.</p> <p>Ilość osób do przeszkolenia: 2.</p> <p>Forma szkolenia: stacjonarne lub online.</p>