

CZĘŚĆ I

Szczegółowy opis przedmiotu zamówienia - Zadanie częściowe nr 1, pozycja 1 Zestaw: System kopii zapasowych - oprogramowanie do tworzenia kopii zapasowych, dedykowane urządzenie dyskowe do bezpiecznego przechowywania kopii zapasowych, wdrożenie	
Zarządzanie i magazyny	- Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2024r. - System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu. - Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe: - Obudowa rack rozmiar: 2U - Procesor: min. 8 rdzeni, min. 16 wątków. Minimalna częstotliwość bazowa procesora 2.8GHz - Pamięć RAM: 32GB DDR4 - Przestrzeń dostępna na przechowywanie danych: Min. 40TB po RAID 6 - Osobne dyski SSD M.2 NVMe działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego, - Redundantne zasilanie, - Interfejsy sieciowe Min. 2szt. Ethernet 1Gb, Dual SFP+ - Gwarancja NBD on-premise (zapewniająca czas reakcji następnego dnia biznesowego obejmująca naprawę w lokalizacji wdrożenia sprzętu) o czasie trwania analogicznym do trwania wsparcia technicznego dla oprogramowania, minimum do dnia 21.06.2026 - Produkt dostępny w polskiej wersji językowej. - Konsola zarządzająca dostępna z poziomu przeglądarki internetowej - System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków - System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów - System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych - System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT - System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft - Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe - System zarządzania nie może być oparty o relacyjne bazy danych. - Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej). - Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów). - Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych. - Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych. - System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle. - System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami. - System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej. - Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie. - Rozwiązanie zapewnia backup jednorzbiegowy - nawet w przypadku wymagania granularnego odtworzenia. - System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu. - Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych - Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów

	PRE/POST oraz po wykonaniu migawki VSS. 25. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego. 26. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii). 27. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane. 28. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione. 29. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika, 30. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta. 31. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym. 32. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych). 33. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych. 34. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów. 35. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych 36. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie. 37. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta. 38. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego. 39. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki. 40. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu. 41. System musi pozwalać na automatyczne aktualizacje oprogramowania. 42. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS. 43. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia. 44. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmiennność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji. 45. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany. 46. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane. 47. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników. 48. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych. 49. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w
--	--

	momencie spełnienia dodatkowych wymogów. 50. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania. 51. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego. 52. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych. 53. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. 54. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental, 55. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC). 56. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3 oraz dedykowana chmura producenta appliance'u 57. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb,S3, nfs, iscsi, katalog lokalny 58. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS). 59. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniem zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu. 60. Możliwość generowania raportów dobowych w oparciu o harmonogram 61. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter powinno być zlokalizowane na terenie Polski) 62. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna) 63. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP. 64. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu)
Wspierane systemy	Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy: Alpine 3.10+, Debian: 9+, Ubuntu: 16.04+, Fedora: 29+, centOS: 7+, RHEL: 6+, openSUSE: 15+, SUSE Enterprise Linux(SLES): 12 SP2+, macOS: 10.13+, Windows: 7, 8.1, 10(1607+), 11 Windows Server: 2008 R2+, Środowisk wirtualnych: Hyper-V 2016+, VMware: 6.7+.
Środowiska fizyczne i bazy danych	1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami. 2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń. 3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej. 4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption. 5. System jest niezależny od wersji Microsoft SQL, PostgreSQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.

	- System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego skalania danych. - System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux. - W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem. - Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika. - Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych. - Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V. - Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK). - Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych. - Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).
Środowiska wirtualne	- System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów. - System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowaniem zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych. - System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych. - Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner. - System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych. - Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna). - System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere. - System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku
Aplikacje SaaS	- Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza. - Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji) - System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365. - System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi - System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe. - System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git. - System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium. - System musi umożliwiać zabezpieczenie środowisk Jira - System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.

Licencjonowanie i wsparcie techniczne	1. Wszystkie linie supportu muszą być obsługiwane w języku polskim. 2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta. 3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu. 4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów) 5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego. 6. W ramach wsparcia technicznego Zamawiający musi mieć dostęp do tzw. Dedicated Customer Success Managera, tj. osoby po stronie Dostawcy dedykowanej do obsługi zgłoszeń technicznych, dorażnej pomocy i bieżącej pomocy w utrzymaniu infrastruktury Zamawiającego. 7. W ramach dokumentacji posprzedażowej Dostawca musi dostarczyć bezpośredni numer telefonu oraz adres e-mail do Dedicated Customer Success Managera. 8. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych. 9. Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu. 10. Wsparcie techniczne producenta na oprogramowanie musi zostać dostarczone na okres min. do 21 czerwca 2026. 11. Licencje muszą umożliwiać replikację na własne zasoby
Anty-ransomware i bezpieczeństwo	1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików"). 2. System powinien umożliwiać wykorzystanie wbudowanego menadżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System 3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty. 4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii. 5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczonym urządzeniu.
Szkolenie	1. Szkolenie musi zostać przeprowadzone w języku polskim, dopuszcza się formę zdalną. 2. Szkolenie jest realizowane bezpośrednio przez producenta oferowanego systemu backupowego. 3. Szkolenie musi zostać przeprowadzone przez dedykowanego inżyniera producenta systemu backupowego. 4. Szkolenie musi zakończyć się imiennym certyfikatem dla administratorów uczestniczących w szkoleniu. 5. Szkolenie musi trwać minimum 8 godzin.
Wdrożenie	1. Wdrożenie zdalne musi zostać realizowane bezpośrednio przez producenta oferowanego systemu backupowego. 2. Wdrożenie musi zostać przeprowadzone przez dedykowanego inżyniera od producenta systemu backupowego. 3. Wdrożenie musi zakończyć się dostarczeniem dokumentacji powdrożeniowej, przygotowanej przez dedykowanego inżyniera od producenta systemu backupowego. 4. Zamawiający powinien móc skorzystać z przynajmniej 6h pomocy wdrożeniowej bezpośrednio świadczonej przez producenta rozwiązania. 5. Wdrożenie powinno być zrealizowane tak, aby dostosować się do preferencji zamawiającego
Szafa teleinformatyczna, UPS	1. Szafa teleinformatyczna 15U 600x800 Budowa: Korpus, osłona tylna, kątowniki nośne - blacha stalowa, drzwi - szkło hartowane. Stopień ochrony: IP 20 zgodnie z normą PN-EN 60529. Wykończenie powierzchni: Korpus i osłona tylna - farba proszkowa. Kątowniki nośne: minimum dwie pary w rozstawie 19", alucynk. Na wyposażeniu szafy minimum 1 listwa zasilająca. 2. Urządzenie UPS o parametrach jak niżej: Technologia wykonania UPS Online podwójna konwersja Moc pozorna (VA) minimum 2000 Moc rzeczywista (W) minimum 1800 Kształt fali na wyjściu(praca na baterii) Pełna fala sinusoidalna

	Ochrona przed przeciążeniem Wymagana(minimum bezpiecznik i wewnętrzny ogranicznik prądu) Filtr EMI/RFI Wymagany Układ przeciwprzepięciowy (J) Wymagany, minimum 430 Charakterystyka wejścia/wyjścia Nominalne napięcie wejściowe (V) 230 Obsługiwany zakres napięcia wejściowego (V) minimum 165 - 295 Częstotliwość wejściowa(Hz) 50+/-10 ; 60+/-10 Wykrywanie częstotliwości wejściowej Wymagane automatyczne Napięcie przy pracy na baterii (V) 208 +/-1% ; 220 +/-1% ; 230 +/-1% ; 240 +/-1% Częstotliwość przy pracy baterii (Hz) 50+/-0.5% ; 60+/-0.5% Charakterystyka gniazd Rodzaj złącza wejściowego IEC C20 Rodzaj złącza wyjściowego 8 x IEC C13 Charakterystyka baterii Typowy czas przełączenia na baterie (ms) 0 ms Bateria wbudowana Wymagana, czas pracy przy pełnym obciążeniu do 5 min, przy połowie obciążenia do 15 min Bateria wbudowana - wymiana Wymagana obsługa Hot-Swap Ładowanie baterii Typowy czas ładowania do 4 h Bateria rozbudowa Wymagana praca z zewnętrznymi modułami baterii Ilość obsługiwanych modułów baterii Minimum 3 Zarządzanie Sygnalizacja Wymagane alarmy dźwiękowe oraz wyświetlacz LCD Alarmy dźwiękowe Minimum Tryb baterii , Niski poziom baterii , Przeciążenie , Przeładowanie , Przegrzanie, Usterka urządzenia Konfiguracja wybranych parametrów Przez wyświetlacz LCD, minimum ustawienia trybu pracy, baterii Port komunikacyjny USB Wymagany Port wyłącznika awaryjnego EPO Wymagany Dołączone oprogramowanie do zarządzania Wymagane, obsługa platform Windows, Linux, Vmware Zarządzanie przez sieć Wymagana możliwość rozbudowy o zarządzanie HTTP/SNMP, np. poprzez doinstalowanie karty zarządzającej Cechy fizyczne Obudowa Wymagana możliwość instalacji w szafie RACK Konstrukcja obudowy Metalowa Szyny/uchwyty rack Wymagane Rozmiary (szer. x wys. x gł.) (mm) Nie większe niż 438 x 88 x 615 Waga Maksimum 22 kg (urządzenie bez opakowania i akcesoriów) Dane środowiskowe Temperatura robocza (°C) 0 - 40 Względna wilgotność robocza (bez kondensacji) (%) 20 - 90 Rozproszenie ciepła (BTU/hr) Nie więcej niż 670 BTU/hr Certyfikaty Pozostałe wymagane certyfikaty CE, RoHS Gwarancja minimum 2 lata na urządzenie i baterie 3. Wykonawca zapewni montaż urządzeń wymienionych w przedmiocie zamówienia we wskazanym miejscu przez Zamawiającego.
--	--

CZĘŚĆ II

Szczegółowy opis przedmiotu zamówienia - Zadanie częściowe nr 2, pozycja 1 Urządzenie UTM wraz z usługą jego wdrożenia i wsparciem technicznym	
Wymagania Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 10 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps. • 4 gniazdami SFP+ 10 Gbps. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 39 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 33 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 5 Gbps. 6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.5 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.
Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zaporę ogniową klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych.

	Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. 3. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego.

	2. Policy Based Routing (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratorium producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem

	wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Hasel dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o:

	zaakceptowanym ruchu, blokowaniem ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. - Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. - Możliwość włączenia logowania per reguła w polityce firewall. - System zapewnia możliwość logowania do serwera SYSLOG. - Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni).
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.
Opisy do wymagań ogólnych	- Wymaga się, aby produkt pochodził z autoryzowanego kanału sprzedaży. - Dla zapewnienia wysokiego poziomu usług, świadczenie wsparcia technicznego oraz wdrożenie rozwiązania musi być realizowane przez certyfikowanego inżyniera, posiadającego minimum 3 aktywne certyfikaty z poniższych: - Certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci(NS) - Certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa(SO) - Certyfikowany Specjalista w zakresie Dostępu Zero Trust(ZTA) - Certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej(PCS) Nie dopuszcza się łączenia certyfikatów przez dwóch lub więcej inżynierów ze względu na poziom bezpieczeństwa oferowanej usługi. Posiadaniem wymaganych certyfikatów należy wykazać się przed przystąpieniem do wdrożenia. - Wykonawca przeniesie konfigurację z posiadanego przez Zamawiającego urządzenia UTM na nowy.
Gwarancja oraz wsparcie	- System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie zamawiającego, realizowana przez producenta lub autoryzowanego dystrybutora w języku polskim przez okres wymaganej gwarancji. - Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji. Do zamawianego sprzętu Wykonawca zapewni usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie: - obsługa procesu RMA u producenta, - zdalna pomoc w skonfigurowaniu urządzenia do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producenta, - jednorazowa podstawowa konfiguracja platformy realizowana przez inżyniera z najwyższym dostępnym poziomem certyfikacji technicznej producenta, - minimum 3 zdalne konsultacje techniczne z inżynierem posiadającym najwyższy poziom certyfikacji technicznej producenta, - jednorazowa usługa hardeningu konfiguracji w formie zdalnej sesji technicznej mającej na celu przegląd konfiguracji urządzenia i przedstawienie zaleceń rekonfiguracji zgodnie z „dobrymi praktykami” producenta, - dostęp do szkolenia wideo prezentującego najlepsze praktyki współpracy z suportem producenta systemu realizującego funkcję Firewall. Dostęp do usługi powinien być świadczony przez dedykowaną infolinię (należy podać numer telefonu) oraz przez dedykowany moduł internetowy (należy podać adres). Usługa ta ma być świadczona przez podmiot posiadający certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.

Rozszerzone wsparcie serwisowe AHB/SOS	System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie: • Wsparcie telefoniczne zespołu certyfikowanych inżynierów. • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. • Doradztwo w zakresie konfiguracji. • Zdalne wsparcie techniczne. • Pomoc w zakładaniu zgłoszeń serwisowych u producenta. • Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). • Przygotowanie urządzenia do zdalnej konfiguracji. • Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. • Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. • Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich. • Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.
--	---

Szczegółowy opis przedmiotu zamówienia - Zadanie częściowe nr 2, pozycja 2 Serwer plików NAS do przechowywania kopii bezpieczeństwa, wdrożenie	
Procesor	Procesor posiadający min. 4 rdzenie, osiągający w teście PassMark CPU Mark wynik min. 3900 według wyników ze strony https://www.cpubenchmark.net .
Obudowa	Rack 2U o wymiarach, 88,6 × 482,14 × 346,43 mm (wys. x szer. x gł.)
Pamięć RAM	8 GB SO-DIMM DDR4 (1 x 8 GB), możliwość rozszerzenia pamięci do 16GB (2x8GB)
Ilość obsługiwanych dysków	8 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s
Interfejsy sieciowe	2 porty 2,5 Gigabit sieci Ethernet (2,5G/1G/100M) • obsługa VLAN i Jumbo Frame
Porty	2x USB 2.0, 2x USB 3.2 Gen 2, 1x HDMI 1.4b
Wskaźniki LED	HDD 1–8, stan, LAN, rozszerzenie, zasilanie
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0,1,5,5+Spare,6,6+Spare,10 i 10+Spare, RAID50, RAID60. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania Global Spare Disk.
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Szyfrowanie	Możliwość szyfrowania całych woluminów kluczem AES 256 bitów.
System Operacyjny	Apple Mac OS 10.10 or later Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 or later Linux IBM AIX 7, Solaris 10 or later UNIX Microsoft Windows 7, 8, and 10 Microsoft Windows Server 2008 R2, 2012, 2012 R2 and 2016, 2019
Stacja monitoringu	Obsługa do 24 kamer IP (8 licencji domyślnie).
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP

Usługi	Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiające zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog, Virtualization Station
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów
Język GUI	Polski
Gwarancja i serwis	36 miesięcy, producenta
Pobór mocy	Praca: ok. 55 W
System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
Liczba kont użytkowników	4096
Liczba grup	512
Liczba udziałów	512
Max ilość połączeń (CIFS)	1500
Max liczba migawek	1024
Zasilanie	Redundantne 300 W (x2), 100–240 V
Wentylatory	2
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.
Dyski	Min. 8 szt. dysków o pojemności 10TB, SATA III (6Gb/s), 7200RPM, 256MB cache, 2mln MTBF, gwarancja producenta 5 lat, prędkość transferu interfejsu na poziomie 273MB/s, w razie awarii uszkodzony dysk zostaje u Zamawiającego

Szczegółowy opis przedmiotu zamówienia - Zadanie częściowe nr 2, pozycja 3 Przełącznik sieciowy	
Przełącznik sieciowy	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.
Parametry fizyczne platformy	• Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. • Zasilanie AC 230V. • Maksymalny pobór mocy: 60 W. • Minimalny zakres temperatury pracy: 0-40°C.
Interfejsy sieciowe - wymagania minimalne	1. Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: a) 48 porty GE RJ-45. e) 4 porty 10 GE SFP+.
Zarządzanie	• Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). • Wsparcie dla SNMP w wersjach 1-3 • Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. • Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. • Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. • Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). • Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.

	• Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. • Automatycznie wykonywane rewizje konfiguracji.
Parametry wydajnościowe	• Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. • Tablica adresów MAC o pojemności co najmniej 32k wpisów. • Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
Wymagane funkcje	• Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. • Obsługa Jumbo Frames. • Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). • Agregacja portów zgodna ze standardem 802.3ad. • Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. • Obsługa routingu statycznego. • Port-mirroring. • Uwierzytelnianie 802.1x na poziomie portu. • Uwierzytelnianie 802.1x w oparciu o adres MAC. • W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). • W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. • W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. • Obsługa protokołu sFlow.
Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: • Centralne zarządzanie konfiguracją urządzenia • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania • Centralne zarządzanie sieciami VLAN. • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. • Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. • Automatyczna detekcja i rekomendacje konfiguracji. • Przesyłanie logów na zewnętrzny serwer syslog. • Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. • Obsługa białych i czarnych list adresów MAC. • Wykrywanie aplikacji komunikujących się w sieci. 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
Akcesoria dodatkowe	Wkładka SFP+ 10G RJ45 (kompatybilna z urządzeniem) – 2 sztuki .
Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. • System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Opisy do wymagań ogólnych	1. Wymaga się, aby produkt pochodził z autoryzowanego kanału sprzedaży. 2. Dla zapewnienia wysokiego poziomu usług, świadczenie wsparcia technicznego oraz wdrożenie rozwiązania musi być realizowane przez certyfikowanego inżyniera, posiadającego minimum 3 aktywne certyfikaty z poniższych: a) Certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci(NS)

	b) Certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa(SO) c) Certyfikowany Specjalista w zakresie Dostępu Zero Trust(ZTA) d) Certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej(PCS) Nie dopuszcza się łączenia certyfikatów przez dwóch lub więcej inżynierów ze względu na poziom bezpieczeństwa oferowanej usługi. Posiadaniem wymaganych certyfikatów należy wykazać się przed przystąpieniem do wdrożenia.
Rozszerzone wsparcie serwisowe	1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy. 2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5.

Szczegółowy opis przedmiotu zamówienia - Zadanie częściowe nr 2, pozycja 4 Serwer z systemem operacyjnym	
Obudowa	- Obudowa Rack o wysokości 2U 8 wnęk na dyski 3.5" - Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej - Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	- Płyta główna z możliwością zainstalowania do dwóch procesorów. - Obsługa procesorów 32 rdzeniowych. - Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. - Na płycie głównej powinno znajdować się 16 slotów przeznaczonych do instalacji pamięci. - Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 169 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	128GB DDR5 RDIMM 5600MT/s,
Kontroler RAID	- Sprzętowy kontroler dyskowy, posiadający - Min. 8GB nieulotnej pamięci cache, - Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. - Wsparcie dla dysków samoszyfrujących
Dyski twarde	- Zainstalowane: 4x dysk SAS o pojemności min. 2.4TB, Hot-Plug - Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
Gniazda PCI	Cztery sloty PCIe
Interfejsy sieciowe/FC/SAS	- Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) - Czteroportowa karta sieciowa 10Gb Ethernet w standardzie BaseT
Wbudowane porty	4 porty USB w tym min: 1 port USB 3.0 z tyłu obudowy, 1 port micro USB z przodu obudowy 2 port VGA z czego jeden z przodu obudowy - Możliwość rozbudowy o port RS232
Video	Zintegrowana karta graficzna umożliwiającą wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne, Hot-Plug

Zasilacze	Redundantne, Hot-Plug min. 700W klasy Titanium
Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
System operacyjny/dodatkowe oprogramowanie	Windows Server 2025 Standard lub równoważny przeznaczony do zarządzania infrastrukturą IT, aplikacjami i usługami, oferujący zaawansowane funkcje bezpieczeństwa, wirtualizacji i integracji z chmurą.
Bezpieczeństwo	- Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardej. - Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. - Możliwość wyłączenia w BIOS funkcji przycisku zasilania. - BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła - Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. - Moduł TPM 2.0 - Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera - Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem - Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	- Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; - możliwość podmontowania zdalnych wirtualnych napędów; - wirtualną konsolę z dostępem do myszy, klawiatury; - wsparcie dla IPv6; - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; - integracja z Active Directory; - możliwość obsługi przez dwóch administratorów jednocześnie; - wsparcie dla automatycznej rejestracji DNS - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. - możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera - możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera - oraz z możliwością rozszerzenia funkcjonalności o: - Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej - Przesyłanie danych telemetrycznych w czasie rzeczywistym - Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze - Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	- Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: - Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych - integracja z Active Directory

	○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejścia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń

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

	▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. • Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: ○ Możliwości utworzenia zgłaszania 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. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń.
--------------------------	---