Postępowanie znak 01/GK/08/26 o udzielenie zamówienia pn „Dostawa i wdrożenie sprzętu informatycznego w ramach projektu oraz doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) wraz z realizacja szkoleń z zakresu cyberbezpieczeństwa" w ramach projektu pn. „Cyberbezpieczne Wodociągi Miejskie Sp. z o.o. w Braniewie"

Załącznik nr 1a do SWZ
Znak 01/GK/08/26

Opis przedmiotu zamówienia – część I

na usługę pn.:

„Dostawa i wdrożenie sprzętu informatycznego w ramach projektu pn. „Cyberbezpieczne Wodociągi Miejskie Sp. z o.o. w Braniewie", finansowanego ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (KPO) Priorytet: C3 Cyberbezpieczeństwo, Działanie C3.1.1. Cyberbezpieczeństwo - CyberPL, konkurs grantowy pn. "Cyberbezpieczne Wodociągi" o numerze KPOD.05.10-CW.01-001/25

Braniewo, dnia: 18.08.2026 r.

Zatwierdza:
Prezes Zarządu

Spis treści

Wstęp i wymagania ogólne

1. Cel i charakter zamówienia Zgodnie z art. 99 ust. 1 ustawy Prawo zamówień publicznych (Pzp), niniejszy przedmiot zamówienia został opisany w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, z uwzględnieniem wszystkich wymagań i okoliczności technicznych mogących mieć wpływ na rzetelne sporządzenie oferty przez Wykonawcę . Głównym celem realizacji zamówienia jest zabezpieczenie oraz optymalizacja infrastruktury informatycznej Zamawiającego poprzez dostarczenie, uruchomienie i zintegrowanie nowoczesnych rozwiązań sprzętowych i programowych.

2. Kompleksowy zakres obowiązków Wykonawcy W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest do kompleksowego świadczenia usług i dostaw , obejmujących nie tylko samą dostawę sprzętu i licencji na oprogramowanie wyszczególnionych w niniejszym dokumencie, ale również pełne wdrożenie operacyjne tych rozwiązań w środowisku Zamawiającego.

Zakres prac powierzonych Wykonawcy obejmuje w szczególności:

- Dostawę i logistykę: Dostarczenie, rozładunek oraz wniesienie fabrycznie nowego sprzętu oraz oprogramowania do wskazanych lokalizacji Zamawiającego, z zachowaniem należytej staranności i zasad bezpieczeństwa transportu urządzeń wrażliwych.
- Wdrożenie i integrację: Przeprowadzenie fizycznej instalacji urządzeń, ich uruchomienie oraz zaawansowaną konfigurację. Wykonawca zobowiązany jest zapewnić bezkolizyjną integrację dostarczanych technologii z istniejącym środowiskiem sieciowo-serwerowym Zamawiającego, minimalizując przy tym ewentualne przerwy w dostępności usług.
- Transfer wiedzy: Przeprowadzenie specjalistycznego instruktażu oraz szkoleń dla personelu technicznego Zamawiającego w zakresie bieżącej obsługi, administracji oraz utrzymania dostarczonych systemów.
- Zgodność z wymaganiami: Pełna realizacja wytycznych, harmonogramu oraz parametrów technicznych określonych szczegółowo w rozdziale *„Wdrożenie dostarczanych rozwiązań wraz z przeszkoleniem"*.

3. Odpowiedzialność za kompletność rozwiązania Wszelkie prace instalacyjne i wdrożeniowe muszą zostać wykonane zgodnie z najlepszymi praktykami rynkowymi, aktualnymi wytycznymi producentów sprzętu i oprogramowania, a także wymogami sztuki inżynierskiej. Wykonawca zobowiązany jest uwzględnić w cenie całkowitej oferty wszystkie koszty niezbędne do prawidłowego, terminowego i kompletnego zrealizowania przedmiotu zamówienia zgodnie z jego przeznaczeniem.

Postępowanie znak 01/GK/08/26 o udzielenie zamówienia pn „Dostawa i wdrożenie sprzętu informatycznego w ramach projektu oraz doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) wraz z realizacja szkoleń z zakresu cyberbezpieczeństwa" w ramach projektu pn. „Cyberbezpieczne Wodociągi Miejskie Sp. z o.o. w Braniewie"

I. Wymagania ogólne dotyczące dostarczanego sprzętu i oprogramowania:

1. Całość dostarczonego sprzętu i oprogramowania musi pochodzić z legalnego źródła, być wprowadzona do obrotu na terytorium Unii Europejskiej zgodnie z prawem i nie może być obciążona prawami osób trzecich.
2. Oferowane urządzenia muszą być fabrycznie nowe, nieużywane, dostarczone w oryginalnych opakowaniach. Niedopuszczalne jest dostarczenie sprzętu naprawianego (odnawianego – tzw. refurbished), pochodzącego z demontażu lub z ekspozycji. Sprzęt musi pochodzić z bieżącej produkcji producenta i na dzień dostawy nie może być obciążony statusem zakończenia sprzedaży lub wsparcia (tzw. End of Sale / End of Life). **Zamawiający traktuje powyższe jako wymagane cechy dostawy niezbędne do właściwej realizacji zamówienia**.
3. Dostarczane licencje na oprogramowanie oraz systemy operacyjne muszą być nowe, niewykorzystywane uprzednio oraz nieaktywowane na innych urządzeniach (Wykonawca dostarczy dokumenty licencyjne wystawione na rzecz Zamawiającego).
4. Sprzęt musi być objęty gwarancją producenta świadczoną na terytorium Rzeczypospolitej Polskiej.
5. Gwarancja musi być realizowana bezpośrednio przez producenta urządzeń lub jego autoryzowaną placówkę serwisową (tzw. gwarancja On-Site u Zamawiającego).
6. Świadczenia gwarancyjne muszą być zapewnione niezależnie od sytuacji prawnej Wykonawcy, w szczególności w przypadku zaprzestania działalności lub niewypłacalności Wykonawcy.
7. Wykonawca oświadcza, że korzystanie przez Zamawiającego z dostarczonych produktów zgodnie z ich przeznaczeniem nie będzie naruszać praw własności intelektualnej ani majątkowych praw autorskich osób trzecich.
8. Cena oferty ujęta w Formularzu Oferty **(rozumiana zgodnie z definicją zawartą w art. 7 pkt 1 ustawy Pzp)** musi obejmować wszystkie koszty związane z realizacją zamówienia, w tym koszty licencji, transportu, ubezpieczenia na czas transportu, wniesienia do wskazanego pomieszczenia Zamawiającego oraz instalacji i wdrożenia.
9. Dostawa zostanie zrealizowana do wskazanych lokalizacji Zamawiającego w dni robocze, w godzinach 8:00-15:00, po uprzednim uzgodnieniu terminu z Zamawiającym.

II. Zasady oceny rozwiązań równoważnych:

10. **Zgodnie z art. 99 ust. 5 ustawy Pzp**, w przypadku, gdy w opisie przedmiotu zamówienia z przyczyn technicznych lub specyfiki przedmiotu znalazły się odniesienia do znaków towarowych, patentów, pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty dostarczane przez konkretnego wykonawcę, **Zamawiający dopuszcza zastosowanie rozwiązań równoważnych opisywanym**.
11. **Wypełniając dyspozycję art. 99 ust. 6 ustawy Pzp**, Zamawiający wskazuje kryteria stosowane w celu oceny równoważności: przez rozwiązanie równoważne Zamawiający rozumie sprzęt lub oprogramowanie o parametrach technicznych, wydajnościowych i funkcjonalnych nie gorszych (tj. takich samych lub lepszych)

niż wskazane w referencyjnym opisie przedmiotu zamówienia, które w pełni umożliwią realizację celu Zamawiającego.

12. Wykonawca, który w ofercie powołuje się na rozwiązania równoważne, **jest obowiązany udowodnić w swojej ofercie, że proponowane przez niego rozwiązania w równoważnym stopniu spełniają wymagania określone przez Zamawiającego**.
13. **Zgodnie z art. 106 ust. 1 w zw. z art. 107 ust. 1 ustawy Pzp, potwierdzenie równoważności musi nastąpić poprzez złożenie wraz z ofertą odpowiednich przedmiotowych środków dowodowych** (np. szczegółowych kart katalogowych producenta, specyfikacji technicznych), z których w sposób niebudzący wątpliwości wynika spełnienie parametrów określonych w opisie przedmiotu zamówienia

Uzasadnienie zamawiającego

Zamawiający dopuścił rozwiązania równoważne, zgodnie z art. 99 ust. 5 i 6 Pzp, a wskazane wymagania mają charakter funkcjonalny i organizacyjny, wynikający z rzeczywistych potrzeb Zamawiającego oraz z konieczności zapewnienia prawidłowej realizacji zamówienia.

Wymóg dostawy sprzętu z bieżącej produkcji, nieobjętego statusem End of Sale / End of Life, jest podyktowany potrzebą zapewnienia długoterminowej dostępności wsparcia producenta, części zamiennych, aktualizacji oraz serwisu, co ma bezpośrednie znaczenie dla bezpieczeństwa eksploatacji i trwałości inwestycji.

Wymóg gwarancji producenta realizowanej w formule On-Site wynika z konieczności ograniczenia przestojów i zapewnienia szybkiej reakcji serwisowej, co jest szczególnie istotne przy urządzeniach wykorzystywanych do wykonywania zadań publicznych i bieżącej pracy Zamawiającego.

Wymogi te nie mają na celu uprzywilejowania jakiegokolwiek wykonawcy lub producenta, lecz służą ochronie interesu Zamawiającego, zapewnieniu jakości i niezawodności dostaw oraz zachowaniu zgodności z zasadami uczciwej konkurencji, równego traktowania wykonawców i proporcjonalności określonymi w art. 16 Pzp.

Dostawa serwera do backupu (testowy serwer odtwarzania kopii) (3.9.2)(3.6.7) (3.11.2) (3.11.3) (3.13.11) (4.7.2)

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
TYP 1 – 1 szt.		W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
1.	**Obudowa**	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.
2.	**Procesor**	Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – 12. Minimalna częstotliwość pracy procesora 2.2GHz. Minimalna ilość kanałów procesora – 8. Wynik wydajności procesora nie powinien być nizszy niż 285 punktów base w teście SPECrate 2017 Integer w teście konfiguracji dwuprocesorowej, opublikowanym przez SPEC.org (www.spec.org), dla ofertowanego serwera.
3.	**Liczba zainstalowanych procesorów**	1
4.	**Płyta główna**	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje
5.	**Pamięć operacyjna**	Zainstalowane minimum 32GB pamięci RAM o częstotliwości 6400MHz. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.
6.	**Zabezpieczenie pamięci**	Memory mirroring, ECC, SDDC, ADDDC
7.	**Procesor Graficzny**	Zintegrowana karta graficzna osiągająca rozdzielczość 1920x1200 przy 60 Hz.
8.	**Dyski**	W chwili dostawy serwer musi posiadać zainstalowane minimum 2 sztuki dysków SSD M.2 NVMe o pojemności przynajmniej 960 GB każdy, sterowane dedykowanym kontrolerem sprzętowym, spięte w RAID1.

		Ponadto musi posiadać zainstalowane min. 4 dyski HDD 2.5" 10k SAS o pojemności 2.4TB każdy, skonfigurowane w RAID5.
9.	**Kontroler dyskowy**	Zainstalowany kontroler dyskowy powinien obsługiwać przynajmniej do 8 sztuk dysków SAS/SATA, posiadać min. 4GB pamięci Cache oraz oferować poziomy zabezpieczeń raid min. 0,1,10,5,50,6,60.
10.	**Zasilacze**	Minimum dwa redundantne zasilacze o mocy minimum 800W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
11.	**Interfejsy sieciowe**	Cztery porty 10G Base-T w jednej karcie niezajmującej slotu PCIe. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
12.	**Sloty I/O**	Min. 2 sloty x16 gen.5
13.	**Dodatkowe porty**	Z przodu obudowy: 2x USB 3 (z czego jeden z możliwością zarządzania serwerem), zewnętrzny dedykowany port diagnostyczny. Z tyłu obudowy: 2x USB 3, 1x VGA, 1x RJ-45 do zarządzania serwerem.
14.	**Chłodzenie**	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
15.	**Zarządzanie**	Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe Porty). Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna Pozyskanie nastepujacych informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarzadzajacej, utylizacja cpu, utylizacja pamięci oraz komponentow I/O, lokalizacja Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. Wysylanie określonych zdarzeń poprzez SMTP oraz SNMPv3 Update systemowego firmware Monitoring i możliwość ograniczenia poboru prądu Zdalne włączanie/wyłączanie/restart Zapis video zdalnych sesji Podmontowanie lokalnych mediow z wykorzystaniem Java client Przekierowanie kosnoli szeregowej przez IPMI Zrzut ekranu w momencie zawieszenia systemu Możliwość przejęcia zdalnego ekranu Możliwość zdalnej instalacji systemu operacyjnego Alerty Syslog Przekierowanie konsoli szeregowej przez SSH

		Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera Możliwość mapowania obrazów ISO z lokalnego dysku operatora Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. Możliwość monitorowania i zarządzania grupą serwerwów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200. Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: - zarzadzanie infrastruktura serwerówi storage bez udziału dedykowanego agenta - przedstawianie graficznej reprezentacji zarządzanych urządzeń - możliwość skalowania do minimum 1000 urządzeń - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2 - wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych - udostępnianie szybkiego podgląd stanu środowiska - udostępnianie podsumowania stanu dla każdego urządzenia - tworzenie alertów przy zmianie stanu urządzenia - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, - konsola zarzadzania oparta o HTML 5 - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostepne na stronie producenta oferowanego rozwiązania - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań - definiowanie roli użytkowników oprogramowania

		- obsługa REST API oraz Windows PowerShell - obsługa SNMP, SYSLOG, Email Forwarding - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML - obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami - przedstawianie historycznych aktywności użytkowników -blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń bedacych w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv - Obsluga NTP - przesyłanie alertów do konsoli firm trzecich - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń) - instalowanie systemów operacyjnych oraz wirtalizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesylem plików diagnostycznych, Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.
16.	**Funkcje zabezpieczeń**	Zainstalowany czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR)., Zainstaloway przedni panel zamykany na klucz. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji.
17.	**Urządzenia hot swap**	Dyski twarde, zasilacze, wentylatory.
18.	**Obsługa**	Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych.

19.	**Diagnostyka**	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID.
20.	**Systemy operacyjne**	• Windows Server 2025 Standard • Dostarczona licencja musi zapewnić pełne pokrycie rdzeni procesora oferowanego serwera.
21.	**Gwarancja**	36 miesiący gwarancji producenta z oknem serwisowym 24x7, z reakcją NBD. Możliwość wykupienia dodatkowego wsparcia, świadczonego przez producenta, z gwarantowanym czasem naprawy w ciągu 24 godzin. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalni jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera. W przypadku awarii dysku po wymianie dysk pozostaje u Zamawiającego.

Dostawa oprogramowania do wykonywania kopii zapasowych (w tym deduplikacji) (3.9.6)(3.11.2) (3.11.3) (3.13.11) (4.7.6)

W ramach dostawy należy dostarczyć taką ilość licencji, aby umożliwiały ochronę min. 15 maszyn wirtualnych.

W ramach dostarczonych licencji musi być możliwość ochrony zarówno maszyn wirtualnych jak i maszyn fizycznych oraz stacji roboczych.

Dostarczone licencje mają upoważniać do użytkowania dostarczonego oprogramowania na czas nieokreślony.

W ramach dostarczonej licencji ma być zapewnione/wykupione roczne wsparcie producenta upoważniające do m.in.:

- aktualizacji oprogramowania do najnowszych wersji bez uiszczania dodatkowych opłat;
- zgłaszania problemów z oprogramowaniem;

Opis techniczny wymagań dotyczących oprogramowania do wykonywania kopii zapasowych:

Oprogramowanie Kopii Zapasowych		
Lp.	**Nazwa parametru, elementu lub cechy**	**Wymagane parametry techniczne**
	1	**2**

Zamawiający wymaga spełnienia przez oprogramowanie minimalnych wymagań w zakresie funkcjonalności określonych poniżej:		
1.	**Wymagania ogólne**	Oprogramowanie musi współpracować z infrastrukturą VMware lub równoważny w wersji 7.x, 8.x i 9.0 oraz Microsoft Hyper-V lub równoważny 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne dla powyższych platform wirtualizacyjnych, chyba, że wyszczególniono inaczej. Oprogramowanie musi współpracować z infrastrukturą Nutanix lub równoważny w wersji 6.8.x - 7.3, Red Hat Virtualization lub równoważny 4.4 SP1, Oracle Linux Virtualization lub równoważny 4.5.5 lub nowszy, Proxmox VE lub równoważny 8.2, 8.3, 8.4 lub 9.0 oraz Scale Computing HyperCore lub równoważny 9.4.32.218226 – 9.5.x. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure lub równoważny, Microsoft Azure Data Lake lub równoważny, AWS S3 lub równoważny i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows lub równoważny i Linux lub równoważny.
2.	**W zakresie funkcjonalności**	System backupowy musi mieć możliwość wdrożenia wszystkich komponentów (np. serwer backupowy, serwer pośredniczący, repozytorium) na platformach Windows lub równoważny oraz Linux lub równoważny System backupowy musi mieć mieć możliwość wdrożenia w oparciu o tzw. appliance zgodny z wytycznymi bezpieczeństwa DISA lub równoważny (Defense Information Systems Agency) Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej

		Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć wiele wirtualnych puli pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej 20 pamięci masowych w pojedyńczej puli. Oprogramowanie musi pozwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob lub równoważny, Google Cloud Storage lub równoważny, Amazon S3 lub równoważny, Wasabi Cloud Storage lub równoważny, IBM Cloud Storage lub równoważny, 11:11 Cloud Storage lub równoważny oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage lub równoważny oraz Amazon S3 Glacier lub równoważny. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania do backupu oraz odtwarzania obrazu maszyny wirtualnej

		Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange lub równoważny i baz danych MS SQL lub równoważny, Oracle lub równoważny oraz PostgreSQL lub równoważny (w tym odtwarzanie point-in-time) Oprogramowanie musi umożliwiać tworzenie logicznie odseparowanych środowisk dla różnych organizacji/działów. Dodatkowo system musi wspierać kontrolę dostępu w oparciu o role (RBAC lub równoważny) - predefiniowane lub własne Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API lub równoważny Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA lub równoważny) w celu dostępu do konsoli administracyjnej Oprogramowanie musi umożliwiać integracje z różnymi dostarczycielami tożsamości (IdP - Identity Providers) z wykorzystaniem protokołu SAML (np. Entra ID lub równoważny, Okta lub równoważny) Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora, reset zablokowanego konta)

		Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS lub równoważny) Oprogramowanie musi posiadać integracje z systemami typu SIEM lub równoważny
3.	**W zakresie RPO**	Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna conajmniej dla platformy VMware lub równoważny i Hyper-V lub równoważny Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware lub równoważny. Oprogramowanie musi posiadać wsparcie dla VMware vSAN lub równoważny potwierdzone odpowiednią certyfikacją VMware lub równoważny. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO lub równoważny oraz IBM 3592 lub równoważny). Oprogramowanie musi mieć możliwość tworzenia retencji GFS lub równoważny (Grandfather-Father-Son) Oprogramowanie musi wspierać BlockClone API lub równoważny w przypadku użycia Windows Server 2016 - 2025 lub równoważny z systemem pliku ReFS lub równoważny jako repozytorium backupu. Podobna funkcjonalność musi być

		zapewniona dla repozytoriów opartych o linuxowy system plików XFS lub równoważny. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere lub równoważny pomiędzy hostami ESXi lub równoważny oraz pomiędzy hostami Hyper-V lub równoważny. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
4.	**W zakresie RTO**	Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware lub równoważny, Hyper-V lub równoważny oraz Nutanix AHV lub równoważny niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dodatkowo dla środowiska vSphere lub równoważny, Hyper-V lub równoważny, Nutanix AHV lub równoważny i MS Azure lub równoważny powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w platformę. Jeżeli licencja na hypervisor nie posiada takich

		funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny, zarówno fizycznej jak i wirtualnej Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL lub równoważny, Oracle lub równoważny i PostgreSQL lub równoważny bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure lub równoważny, Microsoft Azure Stack lub równoważny, Amazon EC2 lub równoważny oraz Google Cloud Platform lub równoważny. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware lub równoważny i PowerShell Direct lub równoważny dla platformy Hyper-V lub równoważny. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows lub równoważny, Linux lub równoważny, BSD lub równoważny, Solaris lub równoważny, Mac lub równoważny, Novell lub równoważny

		Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM Oprogramowanie musi wspierać bezagentowy backup, spójny aplikacyjnie (tzw. Application Consistent) dla maszyn wirtualnych z platfrom vSphere lub równoważny, Hyper-V lub równoważny, Nutanix AHV lub równoważny, Proxmox lub równoważny. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej (Minimum dla Active Directory lub równoważny, MS Exchange lub równoważny, MS SQL lub równoważny, MS Sharepoint lub równoważny, Oracle lub równoważny i PostgreSQL lub równoważny). Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory lub równoważny takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects lub równoważny oraz pozwalać na odtworzenie haseł. Oprogramowanie musi pozwalać na backup i odtwarzanie usługi Entra ID lub równoważny. W szczególności użytkowników, grupy, role, jednostki administracyjne, entrprise applications, Conditional Access Policies lub równoważny, Intune Policies lub równoważny oraz logi audytowe i sign-in. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange lub równoważny (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL lub równoważny. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint lub równoważny. Odtwarzanie musi być możliwe bezpośrednio do środowiska

		produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle lub równoważny z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard lub równoważny. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows lub równoważny oraz Linux lub równoważny. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL lub równoważny z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux lub równoważny. Oprogramowanie musi wspierać granularne odtwarzanie **nierelacyjnej bazy danych** NoSQL lub równoważny przechowującej dane w dokumentach typu JSON lub równoważny (w tym możliwość przywrócenia pojedynczych kolekcji lub dokumentów bez przywracania całej bazy danych). Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowisku Linux lub równoważny. Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA lub równoważny do oryginalnej lub innej lokalizacji Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN lub równoważny Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI lub równoważny Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2 lub równoważny Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN lub równoważny

5.	**W zakresie ograniczenia ryzyka**	Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere lub równoważny i Hyper-V lub równoważny używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) Dla VMware'a lub równoważny oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender lub równoważny, Symantec Protection Engine lub równoważny oraz ESET NOD32 lub równoważny. Oprogramowanie musi posiadać swój wbudowany program antywirusowy zoptymalizowany do przeszukiwania kopii backpowych Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania

		Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków Oprogramowanie musi posiadać mechanizm wykrywania oznak ataku hakerskiego tzw Indicators of Compromise Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk lub równoważny, Palo Alto Networks XSOAR/XSIAM lub równoważny, CrowdStrike Falcon LogScale lub równoważny, Microsoft Sentinel lub równoważny.
6.	**Środowiska Fizyczne**	Rozwiązanie musi wykonywać kopię zapasową systemu Windows lub równoważny oraz Linux lub równoważny wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego Rozwiązanie musi wspierać systemy operacyjne Windows lub równoważny w wersjach klienckich oraz serwerowych Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux lub równoważny: Debian lub równoważny, Ubuntu lub równoważny, RHEL lub równoważny, CentOS lub równoważny, Oracle Linux lub równoważny, SLES lub równoważny, Rocky Linux lub równoważny, AlmaLinux lub równoważny Rozwiązanie musi wspierać system operacyjny macOS lub równoważny Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows lub równoważny, Linux lub równoważny, MacOS lub równoważny, Unix lub równoważny

		Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster lub równoważny Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów Rozwiązanie musi wspierać backup podłączonych dysków USB Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS) lub równoważny, takich jak zewnętrzne dyski USB lub równoważny, eSATA lub równoważny lub Firewire lub równoważny, Network Attached Storage (NAS) lub równoważny pozwalającym na wystawienie swoich zasobów poprzez SMB lub równoważny (CIFS lub równoważny) lub NFS lub równoważny, bezpośrednio na zasobach obiektowych (w tym chmury) Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone Rozwiązanie musi wspierać kontrolę pasma sieciowego Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN

		Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows lub równoważny technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft lub równoważny Rozwiązanie musi wspierać technologię BitLocker lub równoważny Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange lub równoważny, Microsoft Active Directory lub równoważny, Microsoft Sharepoint lub równoważny, Microsoft SQL lub równoważny, Oracle lub równoważny, PostgreSQL lub równoważny oraz MongoDB lub równoważny Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL lub równoważny, Oracle lub równoważny i PostgreSQL lub równoważny poprzez bezpośrednie uruchomienie ich z pliku backupu. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere lub równoważny, Hyper-V lub równoważny, Nutanix AHV lub równoważny, Microsoft Azure lub równoważny, Microsoft Azure Stack lub równoważny, Amazon EC2 lub równoważny oraz Google Cloud Platform lub równoważny Rozwiązanie musi wspierać szyfrowanie Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne

		Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
7.	**Monitoring**	System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere lub równoważny i Microsoft Hyper-V lub równoważny bez potrzeby korzystania z narzędzi firm trzecich System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware lub równoważny w wersji 7.x – 9.0 zarówno w bezpłatnej wersji ESXi lub równoważny jak i w pełnej wersji ESX/ESXi lub równoważny zarządzane przez konsole vCenter Server lub równoważny lub pracujące samodzielnie System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V lub równoważny 2016 – 2025 oraz Azure Stack HCI lub równoważny zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server lub równoważny zarządzane poprzez System Center Virtual Machine Manager lub równoważny lub pracujące samodzielnie. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML lub równoważny oraz Excel lub równoważny

		System musi dawać możliwość podłączenia się do kilku instancji vCenter Server lub równoważny i serwerów Hyper-V lub równoważny jednocześnie, w celu centralnego monitorowania wielu środowisk System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware lub równoważny

8.	**Raportowanie**	System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware lub równoważny w wersji 7.x – 9.0 – zarówno w bezpłatnej wersji ESXi lub równoważny jak i w pełnej wersji ESX/ESXi lub równoważny zarządzane przez konsole vCenter Server lub równoważny lub pracujące samodzielnie System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V lub równoważny 2016 – 2025 oraz Azure Stack HCI lub równoważny zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server lub równoważny zarządzane poprzez System Center Virtual Machine Manager lub równoważny lub pracujące samodzielnie. System musi wspierać wiele instancji vCenter Server lub równoważny i Microsoft Hyper-V lub równoważny jednocześnie bez konieczności instalowania dodatkowych modułów. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V System musi mieć możliwość eksportowania raportów do formatów Microsoft Word lub równoważny, Microsoft Excel lub równoważny, Adobe PDF lub równoważny System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów

		System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware lub równoważny System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie System musi posiadać asystenta produktu opartego o AI lub równoważny, pozwalającego na przeszukiwanie dokumentacji technicznej oraz analizy istniejącej instalacji systemu backupowego. Powinna istnieć możliwość wyłączenia tej opcji.

Dostawa serwera fizycznego pod backup - Serwer typu NAS (3.9.6)(3.6.7) (3.10.2) (3.11.2) (3.11.3) (3.13.11) (4.7.6)

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
TYP 1 – 1 szt.		W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
1.	**Typ**	Serwer typu NAS
2.	**Obudowa**	RACK, max. wysokość 2U
3.	**Backplane**	z min. 8 wnękami na dyski 3.5" SATA
4.	**Procesor**	w architekturze x86, 8 rdzeni , taktowanie min 2,8 GHz
5.	**Liczba zainstalowanych procesorów**	1
6.	**Pamięć operacyjna**	Min. 8GB, DDR4/DDR5
7.	**Rozbudowa pamięci**	Możliwa do min. 64 GB, min. 2 sloty

8.	**Kontroler**	Umożliwiający osiągnięcie poziomów RAID min. 0/1/5/6. Obsługujący dyski SATA.
9.	**Dyski**	Zainstalowane 2 × 8 TB HDD, skonfigurowane w RAID5
10.	**Interfejsy sieciowe**	2 porty 2.5G BASE-T o przepustowości 2.5 Gb/s
11.	**Porty**	Min. 4 porty USB 3.2
12.	**Gwarancja**	3 lata

Dostawa dysków twardych do serwerów (3.9.6)(3.6.7) (3.11.2) (3.13.11) (3.11.3) (4.7.6), w których będą zainstalowane kwalifikowalne systemy z zakresu bezpieczeństwa – 8 sztuk

Dostawa dysków do serwerów S13 lub równoważny o pojemności minimalnie 8 TB HDD.
Dyski muszą być nowe, oryginalne, a także pochodzić z tej samej dystrybucji co wymienione serwery back up'u.
Muszą być kompatybilne z serwerami fizycznymi pod backup oraz monitoring - serwerami typu NAS w bieżącej specyfikacji.

Dostawa UTM (4.1.12) (4.12.5)(4.3.1) (4.2.1) (4.13.1) (3.3.1) (3.4.1) wraz z oprogramowaniem (licencjami) (4.1.12)(4.12.5)(4.3.1) (4.2.1) (4.13.1) (3.4.1) typ I – 2 sztuki

Lp.	**Nazwa parametru, elementu lub cechy**	**Wymagane minimalne parametry techniczne**
	1	**2**

TYP		W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
1.	**Obsługa Sieci**	• Urządzenie ma posiadać wsparcie dla protokołu IPv4 lub równoważny oraz IPv6 lub równoważny co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP lub równoważny. •
2.	**Zapora Korporacyjna (Firewall)**	• Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection lub równoważny. • Urządzenie ma obsługiwać translacje adresów NAT lub równoważny n:1, NAT lub równoważny 1:1 oraz PAT lub równoważny. • Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 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. • 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 lub równoważny), użytkownika bądź grupy z bazy LDAP lub równoważny, pola DSCP lub równoważny nagłówka pakietu, przypisania kolejki QoS lub równoważny, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. • Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. • Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. • Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. • Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP lub równoważny (wewnętrzną

		oraz zewnętrzną), zewnętrzny serwer RADIUS lub równoważny, zewnętrzny serwer Kerberos lub równoważny. • Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). • System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
3.	**Intrusion Prevention System (IPS)**	• 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. • Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. • Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. • Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. • Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML lub równoważny oraz • JavaScript lub równoważny żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. • Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL lub równoważny, co najmniej w zakresie analizy HTTPS lub równoważny, POP3S lub równoważny oraz SMTPS lub równoważny. • Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS lub równoważny, IDS lub równoważny lub Firewall lub równoważny dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP lub równoważny. • Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection lub równoważny, Cross Site Scripting (XSS) lub równoważny oraz złośliwym kodem Web2.0 lub równoważny. • Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus lub równoważny, UMAS lub równoważny, S7 200-300-400 lub równoważny, EtherNet/IP lub równoważny, CIP lub równoważny, OPC UA lub równoważny, OPC (DA/HDA/AE) lub równoważny, BACnet/IP

		lub równoważny, PROFINET lub równoważny, SOFBUS/LACBUS lub równoważny, IEC 60870-5-104 lub równoważny, IEC 61850 (MMS, Goose & SV) lub równoważny. • Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
4.	**Kształtowanie Pasma (Traffic Shapping)**	• 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.
5.	**Ochrona Antywirusowa**	• 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. • Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania). • 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.

6.	**Ochrona Antyspam**	• Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
		• Ochrona antyspam ma działać w oparciu o:
		  ○ 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.
		• Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

7.	**Wirtualne Sieci Prywatne (VPN)**	• Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub siteto-site (lokalizacja-lokalizacja). • Urządzenie ma wspierać co najmniej następujące typy sieci VPN: ○ IPSec VPN lub równoważny, ○ SSL VPN lub równoważny. • SSL VPN ma działać w trybie tunelu. • Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. • 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). • W ramach licencji dostępny jest klient SSLVPN lub równoważny pod systemy: Windows lub równoważny, Linux lub równoważny, macOS lub równoważny objęty gwarancją i wsparciem równolegle ze wsparciem dla rozwiązania UTM. • Urządzenie ma umożliwiać wsparcie dla technologii XAuth lub równoważny, Hub 'n' Spoke lub równoważny oraz modconf lub równoważny. • Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based lub równoważny oraz Route Based lub równoważny. • Rozwiązanie ma umożliwiać wykorzystanie algorytmów post-kwantowej kryptografii w szyfrowaniu IPSec lub równoważny w standardzie ML-KEM lub równoważny. •
8.	**Filtr dostępu do stron WWW**	• 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: ○ blokowanie dostępu do adresu URL, ○ zezwolenie na dostęp do adresu URL, ○ blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML lub równoważny zdefiniowanej przez administratora.

		• Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. • Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. • Filtr URL musi uwzględniać komunikację po protokole HTTPS lub równoważny. • Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME lub równoważny. • Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. • Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch lub równoważny. •
9.	**Uwierzytelnianie**	• Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: ○ lokalną bazę użytkowników (wewnętrzny LDAP), ○ zewnętrzną bazę użytkowników (zewnętrzny LDAP), ○ usługę katalogową Microsoft Active Directory. ○ Microsoft Entra ID lub równoważny, opartej na protokole OpenID Connect lub równoważny. • Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. • Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: ○ SSL lub równoważny, ○ Radius lub równoważny, ○ Kerberos lub równoważny. • Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. • Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. • Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. • 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 lub równoważny i Microsoft Remote Desktop Services (RDS) lub równoważny.

		• Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). • Wbudowany moduł 2FA lub równoważny musi dawać możliwość wykorzystania haseł TOTP lub równoważny w ramach tuneli SSLVPN lub równoważny, IPSec lub równoważny, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH lub równoważny. • Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA) lub równoważny, 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. •

10.	**Administracja Łączami do Internetu (ISP)**	• Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
		• Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
		  ○ równoważenie względem adresu źródłowego,
		  ○ równoważenie względem połączenia.
		• Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
		• Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
		• Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
		• W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
		• Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP lub równoważny oraz TCP lub równoważny.
		•

11.	**Routing (Trasowanie)**	• Urządzenie ma umożliwiać statyczne trasowanie pakietów. • Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. • Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). • Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2 lub równoważny, OSPF lub równoważny oraz BGP lub równoważny.

		• Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.
12.	**Administracja Urządzeniem**	• Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. • Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP lub równoważny, jak zaszyfrowany protokół HTTPS lub równoważny. • Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. • Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. • 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. • Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH lub równoważny) • Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. • Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS lub równoważny. • Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping lub równoważny, traceroute lub równoważny, nslookup lub równoważny. • Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. • Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. • Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). • System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). • Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. • Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog lub równoważny) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS lub równoważny).

		• Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX lub równoważny.
		• Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
		  ○ manualnego eksportu do pliku w dowolnym momencie czasu,
		  ○ 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
		• Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
		• Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
		• Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

13.	**Raportowanie**	• Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. • System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. • System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. • System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. • System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. • System raportowania ma umożliwiać eksport wyników raportu do formatu CSV lub równoważny. • Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. • Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP lub równoważny w wersji 2 i 3. • Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
14.	**Pozostałe Usługi i Funkcje**	• Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. • Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). • Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. • 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). • Urządzenie ma posiadać usługę DNS Proxy. • Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). • Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. • Urządzenie musi mieć możliwość wykorzystania REST API lub równoważny. • 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 zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
15.	**Gwarancja i Serwis**	• Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. • W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
16.	**Parametry Sprzętowe**	• Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. • Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. • Liczba portów Ethernet 2,5Gbps – min.4. • Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. • Przepustowość Firewall (1518 bajtów UDP) – minimum 8,5Gbps. • Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps. • Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1,8Gbps. • Liczba tuneli VPN IPSec – minimum 200. • Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 200. • Obsługa interfejsów 802.11q (VLAN) – minimum 137. • Liczba równoczesnych sesji – minimum 150 000 i nie mniej niż 25 000 nowych sesji/sekundę. • Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. • Urządzenie nie ma limitu na liczbę użytkowników. • Liczba reguł filtrowania – minimum 1024. • Liczba tras statycznego routingu – minimum 512. • Liczba tras dynamicznego routingu – minimum 10 000. • Urządzenie musi posiadać pasywny system chłodzenia. • Urządzenie ma być przystosowane do pracy w temperaturach od -20oC do +60oC przy wilgotności od 0% do 95% (bez kondensacji).

		• Średni czas bezawaryjnej pracy (MTBF) w temperaturze 25 oC ma być nie mniejszy niż 50,1 lat. • Urządzenie musi być przystosowane do montażu na szynie DIN zgodnej ze standardem EN 50022. • Urządzenie musi być wyposażone w moduł TPM. • Urządzenie musi dawać możliwość podłączenia zasilania bezpośrednio z linii produkcyjnej prądem stałym 12-48VDC 3-0,75A. • Urządzenie musi być wyposażone w zasilacz umożliwiający podłączenie do sieci 100-240V 60-50Hz 1,2A.

Dostawa UTM (4.1.12)(4.12.5)(4.3.1) (4.2.1) (4.13.1) (3.3.1) (3.4.1) wraz z oprogramowaniem (licencjami) (4.1.12)(4.12.5)(4.3.1) (4.2.1) (4.13.1) (3.4.1) - typ II

Lp.	**Nazwa parametru, elementu lub cechy**	**Wymagane minimalne parametry techniczne**
	1	**2**
TYP		W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
1.	**Obsługa Sieci**	• Urządzenie ma posiadać wsparcie dla protokołu IPv4 lub równoważny oraz IPv6 lub równoważny co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP lub równoważny. •
2.	**Zapora Korporacyjna (Firewall)**	• Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection lub równoważny. • Urządzenie ma obsługiwać translacje adresów NAT lub równoważny n:1, NAT lub równoważny 1:1 oraz PAT lub równoważny. • Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).

		• 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. • 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 lub równoważny), użytkownika bądź grupy z bazy LDAP lub równoważny, pola DSCP lub równoważny nagłówka pakietu, przypisania kolejki QoS lub równoważny, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. • Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. • Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. • Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. • Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP lub równoważny (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS lub równoważny, zewnętrzny serwer Kerberos lub równoważny. • Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). • System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
3.	**Intrusion Prevention System (IPS)**	• 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. • Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. • Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. • Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. • Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML lub równoważny oraz JavaScript lub równoważny żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.

		• Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL lub równoważny, co najmniej w zakresie analizy HTTPS lub równoważny, POP3S lub równoważny oraz SMTPS lub równoważny. • Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS lub równoważny, IDS lub równoważny lub Firewall lub równoważny dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP lub równoważny. • Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection lub równoważny, Cross Site Scripting (XSS) lub równoważny oraz złośliwym kodem Web2.0 lub równoważny.21. Moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus lub równoważny, UMAS lub równoważny, S7 200-300-400 lub równoważny, EtherNet/IP lub równoważny, CIP lub równoważny, OPC UA lub równoważny, OPC (DA/HDA/AE) lub równoważny, BACnet/IP lub równoważny, PROFINET lub równoważny, SOFBUS/LACBUS lub równoważny, IEC 60870-5-104 lub równoważny, IEC 61850 (MMS, Goose & SV) lub równoważny. • Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
4.	**Kształtowanie Pasma (Traffic Shapping)**	• 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.
5.	**Ochrona Antywirusowa**	• 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. • Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania). • 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.

6.	**Ochrona Antyspam**	• Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
		• Ochrona antyspam ma działać w oparciu o:
		  ○ 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.
		• Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

7.	**Wirtualne Sieci Prywatne (VPN)**	• Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub siteto-site (lokalizacja-lokalizacja).
		• Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
		  ○ IPSec VPN lub równoważny,
		  ○ SSL VPN lub równoważny.
		• SSL VPN ma działać w trybie tunelu.40. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
		• 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).
		• W ramach licencji dostępny jest klient SSLVPN lub równoważny pod systemy: Windows lub równoważny, Linux lub równoważny, macOS lub równoważny objęty gwarancją i wsparciem równolegle ze wsparciem dla rozwiązania UTM.

		• Urządzenie ma umożliwiać wsparcie dla technologii XAuth lub równoważny, Hub 'n' Spoke lub równoważny oraz modconf lub równoważny. • Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based lub równoważny oraz Route Based lub równoważny. • Rozwiązanie ma umożliwiać wykorzystanie algorytmów post-kwantowej kryptografii w szyfrowaniu IPSec lub równoważny w standardzie ML-KEM lub równoważny. •
8.	**Filtr dostępu do stron WWW**	• 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: o blokowanie dostępu do adresu URL, o zezwolenie na dostęp do adresu URL, o blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML lub równoważny zdefiniowanej przez administratora. • Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. • Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. • Filtr URL musi uwzględniać komunikację po protokole HTTPS lub równoważny. • Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME lub równoważny. • Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. • Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch lub równoważny. •
9.	**Uwierzytelnianie**	• Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: o lokalną bazę użytkowników (wewnętrzny LDAP),

		○ zewnętrzną bazę użytkowników (zewnętrzny LDAP), ○ usługę katalogową Microsoft Active Directory. ○ Microsoft Entra ID lub równoważny, opartej na protokole OpenID Connect lub równoważny. • Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. • Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: ○ SSL lub równoważny, ○ Radius lub równoważny, ○ Kerberos lub równoważny. • Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. • Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. • Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. • 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 lub równoważny i Microsoft Remote Desktop Services (RDS) lub równoważny. • Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). • Wbudowany moduł 2FA lub równoważny musi dawać możliwość wykorzystania haseł TOTP lub równoważny w ramach tuneli SSLVPN lub równoważny, IPSec lub równoważny, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH lub równoważny. • Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA) lub równoważny, 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. •

10.	**Administracja Łączami do Internetu (ISP)**	• Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
		• Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
		  ○ równoważenie względem adresu źródłowego,
		  ○ równoważenie względem połączenia.
		• Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
		• Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
		• Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
		• W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
		• Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP lub równoważny oraz TCP lub równoważny.
		•

11.	**Routing (Trasowanie)**	• Urządzenie ma umożliwiać statyczne trasowanie pakietów. • Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. • Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). • Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2 lub równoważny, OSPF lub równoważny oraz BGP lub równoważny. • Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.
12.	**Administracja Urządzeniem**	• Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. • Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP lub równoważny, jak zaszyfrowany protokół HTTPS lub równoważny. • Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. • Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. • 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.

		• Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH lub równoważny)
		• Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
		• Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS lub równoważny.
		• Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping lub równoważny, traceroute lub równoważny, nslookup lub równoważny.
		• Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
		• Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
		• Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
		• System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
		• Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
		• Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.
		• Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog lub równoważny) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS lub równoważny).
		• Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX lub równoważny.
		• Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
		  ○ manualnego eksportu do pliku w dowolnym momencie czasu,
		  ○ 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
		• Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
		• Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
		• Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

13.	**Raportowanie**	• Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. • System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. • System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. • System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. • System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. • System raportowania ma umożliwiać eksport wyników raportu do formatu CSV lub równoważny. • Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. • Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP lub równoważny w wersji 2 i 3. • Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
14.	**Pozostałe Usługi i Funkcje**	• Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP lub równoważny.111. Urządzenie ma posiadać wbudowany serwer DHCP lub równoważny z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. • Urządzenie ma pozwalać na przesyłanie zapytań DHCP lub równoważny do zewnętrznego serwera DHCP lub równoważny (tzw. DHCP Relay lub równoważny). • Konfiguracja serwera DHCP lub równoważny ma być niezależna dla IPv4 lub równoważny i IPv6 lub równoważny. • Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP lub równoważny dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN lub równoważny) w zakresie określenia bramy, serwerów DNS lub równoważny, nazwy domeny). • Urządzenie ma posiadać usługę DNS Proxy lub równoważny.

		• Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP) lub równoważny. • Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN lub równoważny. • Urządzenie musi mieć możliwość wykorzystania REST API lub równoważny. • 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 zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
15.	**Gwarancja i Serwis**	• Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. • W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
16.	**Parametry Sprzętowe**	• Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. • Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. • Liczba portów Ethernet 2,5Gbps – min. 8. • Liczba portów światłowodowych 1Gbps – min. 1. • Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. • Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps. • Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 6Gbps. • Przepustowość typu Threat Prevention – minimum 740Mbps. • Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 3Gbps. • Liczba tuneli VPN IPSec – minimum 300. • Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 300. • Obsługa interfejsów 802.11q (VLAN) – minimum 393. • Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 39 000 nowych sesji/sekundę. • Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive przy zakupie drugiego takiego urządzenia (dostawa drugiego urządzenia nie jest wymagana). • Urządzenie nie ma limitu na liczbę użytkowników. • Liczba reguł filtrowania – minimum 8 192. • Liczba tras statycznego routingu – minimum 512. • Liczba tras dynamicznego routingu – minimum 10 000.

		• Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia. • Urządzenie musi być wyposażone w moduł TPM.

Dostawa i wdrożenie oprogramowania typu SIEM (4.1.12)(4.12.8) (4.3.17) (4.10.1) (4.10.2) (4.11.1) (4.11.2) (3.4.16)

Lp.	**Nazwa parametru, elementu lub cechy**	**Wymagane minimalne parametry techniczne**
	1	**2**
TYP		W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
17.	**Wymagania ogólne**	• Platforma bezpieczeństwa łącząca funkcje SIEM oraz XDR, przeznaczona do monitorowania bezpieczeństwa endpointów, serwerów, środowisk lokalnych, wirtualnych, kontenerowych i chmurowych • Rozwiązanie umożliwia zbieranie i analizę zdarzeń bezpieczeństwa, wykrywanie zagrożeń, monitorowanie integralności plików, analizę podatności, kontrolę konfiguracji bezpieczeństwa. • System musi wykorzystywać skalowalny, wyspecjalizowany silnik indeksowania logów, (wymagana kompatybilność z silnikiem OpenSearch lub równoważny) umożliwiający pełnotekstowe wyszukiwanie, filtrowanie, agregacje i wysoką przepustowość. • System musi być skalowalny, umożliwiając w przyszłości rozbudowę o dodatkowe węzły. • Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej (architektura x86-64) i dyskowej. • System musi być produktem posiadającym aktywne wsparcie społeczności lub producenta • Architektura musi umożliwiać łatwe i niezależne skalowanie komponentów odpowiadających za przetwarzanie logów, wyszukiwanie oraz przechowywanie danych.

18.	**Zbieranie i obsługa logów**	• System musi umożliwiać centralne zbieranie i analizę zdarzeń z: ○ systemów operacyjnych stacji roboczych i serwerów (zarówno z rodziny Microsoft Windows lub równoważny, jak i Unix/Linux lub równoważny), ○ aktywnych urządzeń sieciowych warstwy dostępowej i rdzeniowej (przełączniki sieciowe, routery), ○ rozwiązań bezpieczeństwa sieciowego klasy NGFW (Next-Generation Firewall), UTM oraz systemów ochrony aplikacji webowych (WAF), ○ urządzeń infrastruktury technicznej i serwerowej, w tym sieciowych pamięci masowych (NAS) oraz systemów zasilania gwarantowanego i dystrybucji zasilania (UPS, listwy zarządzalne PDU), ○ systemów ochrony stacji końcowych klasy EPP/EDR (Endpoint Protection Platform / Endpoint Detection and Response) lub równoważny, w zakresie zdarzeń bezpieczeństwa i wykryć antywirusowych. • Zamawiający wymaga, aby zaoferowane rozwiązanie było niezależne od producentów źródeł danych i umożliwiało integrację z dowolnym urządzeniem wysyłającym logi w standardach branżowych opisanych w wymaganiu poniżej • System musi umożliwiać przyjmowanie danych z wykorzystaniem standardowych protokołów i formatów, w tym Syslog UDP/TCP lub równoważny, SNMP Trap lub równoważny, HTTP/HTTPS API lub równoważny, Raw TCP/UDP lub równoważny, odczytu z plików płaskich oraz formatów ustrukturyzowanych, takich jak JSON lub równoważny, XML lub równoważny, CEF lub równoważny, LEEF lub równoważny lub równoważnych, a także logów nieustrukturyzowanych. • System musi posiadać mechanizm do buforowania (kolejkowania) przychodzących logów w celu ochrony przed utratą danych w przypadku chwilowego przeciążenia indeksowania (np. użycie Apache Kafka lub równoważny, RabbitMQ lub równoważny lub wbudowanego mechanizmu buforowania dyskowego tzw. Journal). • System musi umożliwiać definiowanie dowolnych portów nasłuchu logów dla każdego źródła danych. • Konfiguracja systemu musi pozwalać na swobodną kategoryzację napływających danych, umożliwiając wydzielenie dedykowanych kanałów przetwarzania tzw. strumieni dla poszczególnych klas

		infrastruktury IT (w tym dla systemów operacyjnych, sieci i systemów bezpieczeństwa). • System musi posiadać funkcjonalność automatycznej konwersji stref czasowych logów (np. z UTC do lokalnej), aby zapewnić spójność danych. • System musi przechowywać zdarzenia w postaci umożliwiającej analizę, wyszukiwanie i korelację, tj. po przetworzeniu, normalizacji i parsowaniu do pól. Jednocześnie system powinien umożliwiać dostęp do oryginalnej treści logu źródłowego lub jej reprezentacji w rekordzie zdarzenia, w celu weryfikacji i analizy szczegółowej • System musi umożliwiać wzbogacanie logów o dane kontekstowe (np. geolokalizację, DNS, dane o użytkownikach). • System musi posiadać możliwość eksportu i importu danych (Content Packs lub równoważne paczki konfiguracyjne) oraz konfiguracji ekstraktorów i dashboardów.
19.	**Wizualizacja i raportowanie**	• System musi umożliwiać tworzenie dashboardów w formie graficznej i tabelarycznej, obejmujących dane ze wszystkich źródeł • Wszystkie widoki muszą posiadać mechanizm szybkiego filtrowania czasowego np. ostatnie 15 min, dowolny zakres, oraz możliwość zapisywania widoków
20.	**Alerty i powiadomienia**	• System musi umożliwiać podstawowe alarmowanie oparte regułach, progach i agregacji zdarzeń, np. wygenerowanie alarmu po przekroczeniu określonej liczby zdarzeń i/lub po wystąpieniu zdarzenia określonego typu/kategorii.
21.	**Użytkownicy**	• System musi posiadać możliwość ręcznego tworzenia kont użytkowników • System musi posiadać możliwość integracji z Active Directory / LDAP lub równoważny w celu centralnego zarządzania użytkownikami. • System musi wspierać RBAC (Role Based Access Control) lub równoważny pozwalający na definiowanie ról, ograniczanie dostępu do konkretnych strumieni logów/dashboardów oraz realizację zasady minimalnych uprawnień. •
22.	**Wykrywanie podatności**	• System musi posiadać mechanizm wykrywania podatności na monitorowanych agentowo punktach końcowych poprzez inwentaryzację systemu operacyjnego i zainstalowanego oprogramowania oraz korelację wykrytych wersji pakietów/aplikacji z bazami podatności. Wyniki analizy powinny być prezentowane w interfejsie GUI w postaci listy podatności, identyfikatorów CVE, poziomu ryzyka oraz powiązanych zasobów.

Dostawa i wdrożenie oprogramowania do monitorowania typu NDR wraz z wdrożeniem (4.1.12)(4.12.8) (4.3.18) (4.2.4) (4.2.5) (3.3.4) (3.3.5) (3.4.17)

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
TYP		W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
1.	Wymagania ogólne	• System monitorowania infrastruktury, przeznaczony do nadzorowania dostępności, wydajności i stanu pracy serwerów, urządzeń sieciowych, maszyn wirtualnych, aplikacji, baz danych, usług, środowisk chmurowych oraz zasobów systemowych. • Rozwiązanie umożliwia bieżące zbieranie metryk, analizę progów alarmowych, wizualizację danych oraz generowanie powiadomień o awariach, przekroczeniach parametrów lub niedostępności usług
2.	Monitorowanie	• Monitorowanie parametrów systemowych: CPU, RAM, przestrzeń dyskowa, monitorowanie usług • Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń • Możliwość przesyłania danych z monitorowanych systemów za pomocą dedykowanego agenta • Wspierane metody monitorowania: SNMP lub równoważny, IPMI lub równoważny, JMX lub równoważny, HTTP/HTTPS lub równoważny •
3.	Wizualizacja	• Wizualizacja danych: dashboardy, wykresy, mapy
4.	Alerty i powiadomienia	• Definiowanie progów alarmowych wraz z możliwością wysyłki powiadomień e-mail

5.	**Użytkownicy**	• możliwość definiowania kont lokalnych lub integracja z zewnętrznym źródłem tożsamości użytkowników, np. LDAP/Active Directory
6.	**Interfejs użytkownika (GUI)**	• Konfiguracja oprogramowania systemu monitorowania poprzez graficzny interfejs WWW

Dostawa serwera dedykowanego pod monitoring - Serwer typu NAS (4.1.12)(4.3.18) (4.10.10) (4.9.2) (4.9.3) (3.4.17)

Lp.	**Nazwa parametru, elementu lub cechy**	**Wymagane minimalne parametry techniczne**
	1	**2**
TYP 1 – 1 szt.		W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
1.	**Typ**	Serwer typu NAS
2.	**Obudowa**	RACK, max. wysokość 2U
3.	**Backplane**	z min. 8 wnękami na dyski 3.5" SATA
4.	**Procesor**	w architekturze x86, 8 rdzeni , taktowanie min 2,8 GHz
5.	**Liczba zainstalowanych procesorów**	1

6.	**Pamięć operacyjna**	Min. 8GB, DDR4/DDR5
7.	**Rozbudowa pamięci**	Możliwa do min. 64 GB, min. 2 sloty
8.	**Kontroler**	Umożliwiający osiągnięcie poziomów RAID min. 0/1/5/6. Obsługujący dyski SATA.
9.	**Dyski**	Zainstalowane 2 × 8 TB HDD, skonfigurowane w RAID5
10.	**Interfejsy sieciowe**	2 porty 2.5G BASE-T o przepustowości 2.5 Gb/s
11.	**Porty**	Min. 4 porty USB 3.2
12.	**Gwarancja**	3 lata

Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source IT/OT/ICS/IIoT – Wdrożenie systemu monitoringu (instalacja, konfiguracja) (4.1.16) (4.3.27)

Wdrożenie systemu monitoringu (instalacja, konfiguracja) (4.1.16) (4.3.27) wraz z dostawa wieczystych licencji oprogramowania do monitoringu wizyjnego klasy VMS (Video Management Software) / NVR (Network Video Recorder), przeznaczonego do instalacji na serwerze NAS Zamawiającego, wraz z aplikacjami klienckimi (desktop i mobilną), dokumentacją oraz wsparciem technicznym producenta na okres minimum 12 miesięcy.

Wskazane parametry stanowią wymagania minimalne. Wszędzie, gdzie wskazano znaki towarowe lub konkretny standard, Zamawiający dopuszcza rozwiązania równoważne, spełniające co najmniej parametry techniczne i funkcjonalne wskazane w niniejszej specyfikacji.

Lp.	Wymaganie
I. Architektura i licencjonowanie	
1	Oprogramowanie do monitoringu wizyjnego klasy VMS / NVR, instalowane na serwerze NAS Zamawiającego, umożliwiające rejestrację, archiwizację i zarządzanie obrazem z kamer IP.
2	Aplikacja działa w środowisku odizolowanym od systemu operacyjnego NAS (np. w technologii kontenerów lub równoważnej), zapewniając niezależność wydajnościową od pozostałych aplikacji uruchomionych na NAS.
3	Licencja wieczysta (bezterminowa). Subskrypcja czasowa nie będzie akceptowana.
4	W wersji podstawowej (bez dodatkowych licencji) minimum 8 kanałów kamer.
5	Możliwość rozbudowy do co najmniej 128 kanałów na pojedynczej instancji systemu poprzez zakup dodatkowych licencji.
6	Możliwość dodawania pojedynczych kanałów lub pakietów wielokanałowych (np. 1, 4, 8) bez wymiany licencji bazowej.
7	Dedykowana przestrzeń dyskowa rezerwowana wyłącznie na nagrania, niezależna od pozostałych przestrzeni NAS.

Lp.	Wymaganie
8	Możliwość rozbudowy przestrzeni nagrań poprzez moduły rozszerzające pamięć masową oraz wykorzystanie wolnej przestrzeni innych serwerów NAS w sieci (technologia typu virtual JBOD lub równoważna).
II. Obsługa kamer IP	
1	Obsługa kamer IP zgodnych ze standardem ONVIF.
2	Natywne integracje z minimum 150 producentami kamer (lista zgodności publikowana przez producenta), co najmniej takich jak: Axis, Hikvision, Dahua, Bosch, Sony, Panasonic, Vivotek, Hanwha (Samsung) lub równoważnych.
3	Obsługa źródeł obrazu poprzez protokoły strumieniowe RTSP oraz RTMP, bez konieczności posiadania natywnej integracji z kamerą.
4	Możliwość wykorzystania kamer USB jako źródeł obrazu poprzez dedykowaną aplikację producenta.
5	Obsługa kamer panoramicznych (typu rybie oko / fish-eye) z funkcją cyfrowej korekcji zniekształceń (dewarping).
6	Możliwość jednoczesnego wyświetlania obrazu z pojedynczej kamery typu rybie oko w minimum 9 kanałach z różnych perspektyw, bez pogorszenia jakości nagrania.

Lp.	Wymaganie
7	Obsługa kamer 360° / panoramicznych oraz kamer PTZ (pan-tilt-zoom), w tym sterowanie i wywoływanie predefiniowanych pozycji (presetów).
8	Automatyczne wyszukiwanie kamer w sieci oraz dodawanie kamer z różnych podsieci.
9	Zbiorcze dodawanie wielu kamer z możliwością zastosowania wspólnych ustawień dla kamer tego samego modelu/marki.
10	Obsługa minimum kodeków H.264 oraz H.265 (HEVC).
III. Rejestracja i archiwizacja nagrań	
1	Rejestracja ciągła (24/7), wyzwalana zdarzeniem (np. detekcja ruchu, sygnał z wejścia I/O kamery) oraz według harmonogramu.
2	Definiowanie indywidualnej, dedykowanej przestrzeni dyskowej dla nagrań poszczególnych kamer.
3	Ustawienie minimalnej oraz maksymalnej liczby dni przechowywania nagrań indywidualnie dla każdej kamery.
4	Oddzielna alokacja zasobów strumieniowania oraz oddzielnej przestrzeni dyskowej dla nagrań ogólnych (ciągłych) i nagrań zdarzeń (np. zapis zdarzeń na SSD).

Lp.	Wymaganie
5	Definiowanie zapasowego (rezerwowego) woluminu dyskowego, na który automatycznie zapiszą się nagrania w przypadku awarii woluminu podstawowego.
6	Przypisanie dedykowanej przepustowości sieciowej do poszczególnych kamer.
7	Szybki przegląd wszystkich nagrań wraz z informacją o zajętej przestrzeni dyskowej w podziale na kamery.
IV. Aplikacja kliencka – stanowisko operatora (desktop)	
1	Dedykowana aplikacja kliencka do podglądu na żywo i odtwarzania nagrań, dostarczana w ramach licencji.
2	Aplikacja dostępna w wersjach dla systemów: Microsoft Windows (minimum Windows 10, 64-bit) oraz macOS.
3	Jednoczesny podgląd obrazu z wielu kanałów oraz odtwarzanie nagrań w jednym wspólnym interfejsie.
4	Przełączanie pomiędzy trybem podglądu na żywo, trybem odtwarzania pojedynczego oraz trybem odtwarzania zsynchronizowanego (jednoczesnego) wielu kanałów.
5	Przeglądanie nagrań w wybranym przedziale czasowym poprzez kliknięcie na osi czasu (timeline) lub wybór zakresu z kalendarza.

Lp.	Wymaganie
6	Dekodowanie obrazu z przyspieszeniem sprzętowym (GPU karty graficznej lub zintegrowanej grafiki procesora) w celu odciążenia CPU stacji operatora.
7	Konfigurowalny układ panelu wyświetlania, w tym zmiana proporcji kanałów, dynamiczne porządkowanie elementów oraz zapis własnych układów.
8	Funkcja rejestrowania obszarów (focused area) – definiowanie w obrazie z jednej kamery wielu wycinków o szczególnym znaczeniu, dostępnych w trybie podglądu i odtwarzania, bez dodatkowych licencji.
9	Funkcja interaktywnej e-mapy obiektu z możliwością umieszczenia ikon kamer na planie i szybkiego przejścia do podglądu wybranej kamery.
10	Powiadamianie operatora o zdarzeniach minimum poprzez: migające obramowanie kanału, sygnał dźwiękowy oraz ikonę/animację na e-mapie.
11	Szybkie odtwarzanie z możliwością przyspieszenia (np. wielokrotność prędkości) oraz szybkie eksportowanie nagrań do plików.
V. Aplikacja mobilna i klient TV	
1	Aplikacja mobilna do podglądu na żywo i odtwarzania nagrań – wersje na Android oraz iOS (Apple).

Lp.	Wymaganie
2	Układy wielu kanałów oraz szybkie przełączanie pomiędzy trybem na żywo i trybem odtwarzania.
3	Tryb niskiej przepustowości (low-bandwidth) – zoptymalizowany strumień bez wpływu na oryginalne nagranie – do wykorzystania w sieciach o ograniczonym łączu.
4	Sterowanie kamerami PTZ oraz wywoływanie predefiniowanych pozycji (presetów) z poziomu urządzenia mobilnego.
5	Widok kamery z poziomu e-mapy oraz odbieranie powiadomień push o zdarzeniach.
6	Możliwość uruchomienia podglądu i odtwarzania nagrań na urządzeniu typu Apple TV za pomocą dedykowanej aplikacji.
VI. Detekcja zdarzeń i analityka wideo	
1	Obsługa detekcji ruchu wbudowanej w kamerę (po stronie kamery) oraz detekcji ruchu po stronie serwera dla kamer nieposiadających własnej detekcji (w tym kamer USB), z obsługą rozdzielczości minimum do 1080p.
2	Minimum 1 kanał detekcji ruchu po stronie serwera bez konieczności zakupu dodatkowych licencji.
3	Definiowanie obszaru detekcji oraz progu czułości indywidualnie dla każdej kamery.

Lp.	Wymaganie
4	Otwarte API umożliwiające integrację z systemami zewnętrznymi (IoT, czujniki, kontrola dostępu, alarmy) oraz definiowanie reguł alertów wyzwalanych przez systemy zewnętrzne.
VII. Centralne zarządzanie wieloma instancjami (CMS)	
1	Scentralizowane zarządzanie wieloma niezależnymi instancjami systemu zainstalowanymi w różnych lokalizacjach z poziomu jednego interfejsu.
2	Centralna aplikacja zarządzająca umożliwia: jednoczesny podgląd na żywo z wielu lokalizacji, odtwarzanie nagrań z wielu lokalizacji, odbieranie powiadomień o zdarzeniach z wielu lokalizacji.
VIII. Bezpieczeństwo i kontrola uprawnień	
1	Szczegółowe uprawnienia dostępu dla poszczególnych użytkowników i grup użytkowników.
2	Domyślne role: minimum Administrator, Przełożony (Supervisor), Przeglądający (Viewer).
3	Tworzenie nowych, niestandardowych ról ze spersonalizowanym dostępem do określonych: kanałów kamer, układów wyświetlania, e-map, funkcji systemowych.

Lp.	Wymaganie
4	Dziennik zdarzeń (log) zawierający informacje o operacjach wykonywanych przez użytkowników i zdarzeniach systemowych.
IX. Wymagania środowiskowe, wsparcie i dokumentacja	
1	Pełna kompatybilność z serwerem(-ami) NAS Zamawiającego (architektura procesora x86-64 lub ARM 64-bit).
2	Minimalne wymagania pamięciowe: 4 GB RAM. Zalecane: 8 GB RAM lub więcej.
3	Minimum 12-miesięczne wsparcie techniczne oraz prawo do bezpłatnej aktualizacji oprogramowania od daty dostarczenia licencji.
4	Wsparcie obejmuje dostęp do: aktualizacji wersji (w tym poprawek bezpieczeństwa), oficjalnej bazy wiedzy producenta, oficjalnego portalu serwisowego producenta.
5	Interfejs użytkownika dostępny minimum w języku polskim lub angielskim.
6	Wraz z licencją Wykonawca dostarczy: dokumentację techniczną w języku polskim lub angielskim w formie elektronicznej, klucz(e) licencyjne oraz instrukcję ich aktywacji.

Lp.	Wymaganie
7	Oprogramowanie dostępne w oficjalnym kanale dystrybucji producenta na rynek Polski; numer katalogowy (PN) licencji publicznie dostępny w oficjalnym cenniku producenta.

Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source IT/OT/ICS/IIoT – Wdrożenie rozwiązań typu UTM (4.1.16)(4.3.27); SIEM, NDR, Serwery, backup (3.9.8)(4.7.8)

Wszystkie dostarczone urządzenia zostaną podłączone i skonfigurowane zgodnie z aktualną wiedzą techniczną i zaleceniami producenta oraz przez osobę odpowiednio wykwalifikowaną. Prace wdrożeniowe będą obejmowały instalację i konfigurację urządzeń oraz oprogramowania.

Minimalny zakres :

- fizyczny montaż urządzeń w miejscu wskazanym przez Zamawiającego

- podłączenie urządzeń do istniejącej instalacji prądowej
- podłączenie urządzeń do sieci LAN Zamawiającego
- instalacja i konfiguracja UTMów
- instalacja i konfiguracja serwera do wykonywania kopii
- instalacja i konfiguracja systemu kopii zapasowych
- konfiguracja urządzeń firewall
- wykonanie weryfikacji prawidłowego działania dostarczonych urządzeń oraz oprogramowania

Wdrożenie systemu SIEM oraz systemu do monitorowania infrastruktury w zakresie dostarczanych komponentów sprzętowo-programowych wraz z instruktażem zdalnym z administracji systemami (SIEM oraz do monitorowania infrastrkutury IT (typu NDR) obejmującym m.in. zagadnienia dotyczące instalacji agentów i/lub podłączania źródeł bezagentowych (np. syslog lub SNMP)

Dostarczenie wszelkich komponentów potrzebnych do zamontowania dostarczonych urządzeń oraz do połączenia urządzeń do infrastruktury pasywnej (np. przewody krosowe).

Wykonawca po zainstalowaniu wszystkich dostarczonych urządzeń opracuje szczegółową dokumentację techniczną powykonawczą zawierającą dokładny opis montażu, instalacji i konfiguracji zainstalowanych komponentów. Dokumentacja powykonawcza będzie zawierała szczegółowe opisy zastosowanych rozwiązań.

Wymagania dotyczące instruktaż.

Wykonawca na potrzeby wdrożenia zapewni instruktaż z dostarczonych produktów infrastruktury serwerowej.

Wymagania dotyczące zdolności technicznej – znajdują się w dokumencie SWZ - 17.1.4. - Zdolność techniczna lub zawodowa.

Signed by / Podpisano przez:

Bartłomiej Adam Fita

Date / Data: 2026-08-18 12:32