

Załącznik nr 6 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

„Cyberbezpieczny Samorząd”

Dostawa sprzętu i oprogramowania w ramach projektu grantowego

INFORMACJE

Wykonawca zobowiązuje się do:

1. Dostarczenia sprzętu, który jest fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w np. styczniu 2023 r., dostarczony w opakowaniu oryginalnym (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Nie dopuszcza się zastosowania urządzeń tzw. „refurbished”.
2. Towar, będący przedmiotem zamówienia, nie jest również refabrykowany, recertyfikowany, poleasingowy, a każdy oferowany element danej pozycji jest jednakowego producenta, modelu, wersji i specyfikacji.
3. Dostarczenia oprogramowania, które jest nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) musi być wolne od wad fizycznych i prawnych.
4. Dostarczenia przedmiotu zamówienia, który jest fabrycznie nowy, kompletny, oznakowany oraz musi być dopuszczony do obrotu na terytorium Rzeczypospolitej Polskiej. Składana oferta winna obejmować cały zakres rzeczowy i ilościowy zamówienia określony w niniejszej OPZ.

Rozwiązania równoważne:

1. Zgodnie z art. 99 ust. 4 i 5 ustawy Pzp, wszelkie wskazane w OPZ lub załącznikach do OPZ z nazwy urządzenia, materiały lub rozwiązania należy rozumieć jako określenie wymaganych parametrów technicznych lub standardów jakościowych. Oznacza to, że w przypadku wskazania z nazwy materiałów (wyrobów) lub rozwiązań Zamawiający dopuszcza zastosowanie równoważnych rozwiązań lub materiałów nie gorszej jakości niż opisane w OPZ lub załącznikach do OPZ.
2. Ilekroć w OPZ przedmiot zamówienia jest opisany ze wskazaniem znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę jak również norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych oznacza to, że zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób i przyjmuje się, że wskazaniom takim towarzyszą wyrazy „lub równoważne”. Wszelkie ww. wskazania zostały przywołane w celu sprecyzowania parametrów i wymogów technicznych, użytkowych, funkcjonalnych i jakościowych przedmiotu zamówienia.
3. Wykonawca, który powołuje się na rozwiązania równoważne, jest zobowiązany wykazać, że oferowane przez niego materiały/urządzenia/wyroby/rozwiązania spełniają wymagania określone przez Zamawiającego na poziomie nie niższym niż wskazany w opisie przedmiotu zamówienia. W takim przypadku, Wykonawca załącza do oferty wykaz rozwiązań równoważnych wraz z jego opisem lub normami potwierdzającymi tą równoważność.
4. Niewskazanie w ofercie rozwiązań równoważnych traktowane będzie jako deklaracja zastosowania rozwiązań wymienionych w OPZ.
5. Miejsce dostawy zostanie wskazane przez Zamawiającego.
6. Wykonawca zobowiązany jest do zawiadomienia Zamawiającego o terminie dostawy przedmiotu zamówienia
7. Dostawa przedmiotu zamówienia nastąpi na koszt własny Wykonawcy, w opakowaniu firmowym odpowiadającym właściwościom sprzętu komputerowego zapewniającym jego całość i nienaruszalność. W przypadku, gdy przedmiot zamówienia nie jest dostarczany na fizycznym nośniku danych, ale udostępniany w sposób elektroniczny, wówczas przedmiot zamówienia zostanie udostępniony Zamawiającemu w formie linku do miejsca pobrania.
8. Gwarancja obejmuje wszystkie wykryte podczas eksploatacji towaru usterki i wady oraz uszkodzenia powstałe w czasie zgodnego z instrukcją korzystania ze sprzętu.

Informacje dodatkowe:

1. Dodatkowo Zamawiający zastrzega możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów u Producenta w przypadku wystąpienia wątpliwości co do jego legalności.
2. Wszystkie wymagania określone w dokumentach wskazanych powyżej stanowią wymagania minimalne, a ich spełnienie jest obligatoryjne. Niespełnienie ww. wymagań minimalnych będzie

skutkować odrzuceniem oferty, jako niezgodnej z warunkami zamówienia na podstawie art. 226 ust. 1 pkt. 5 ustawy Pzp.

3. Zamawiający zastrzega możliwość niedopuszczenia rozwiązań równoważnych, wszędzie tam, gdzie ze względu na kompatybilność technologii z rozwiązaniami już posiadanymi, mogłoby w jakimkolwiek stopniu ograniczyć funkcjonalność rozwiązań, czy narazić go na jakiegokolwiek dodatkowe koszty, np.: koszty modernizacji, integracji czy koszty szkolenia.
4. Zamawiający informuje, że może żądać od Wykonawcy przedstawienia dodatkowych dokumentów potwierdzających spełnienie wymagań w OPZ dla oferowanego rozwiązania.

Zamówienie część 1

Nr	Nazwa elementu, parametru lub cechy	Parametry wymagane przez Zamawiającego
----	-------------------------------------	--

1	Aktualizacja licencji dla posiadanych UTM (CPV-48219100-7)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanej licencji
	Ilość zamawiana	Licencje UTP dla 2 posiadanych urządzeń UTM Fortigate 60F
	Typ licencji	Licencja przedłużenia wsparcia i gwarancji producenta na okres 1 roku (Unified Threat Protection UTP FC-10-0060F-950-02-12) dla posiadanych przez Zamawiającego urządzeń FortiGate 60F

2	Zakup urządzeń UTM wraz z licencjami oraz wsparciem i gwarancją (CPV-32410000-0)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia i licencji
	Ilość zamawiana	2 urządzenia UTM z licencjami
	Opis	Zapora UTM, która realizuje: kontrolę aplikacji, IPS, VPN, web filtering oraz firewall z dostępem do aktualizowanych serwisów, zapewniających automatyczną ochronę w czasie rzeczywistym

	Interfejsy	1xWAN, 4xLAN, 1xUSB
	Przepustowość IPS	1 Gb/s
	Przepustowość firewalla	5 Gb/s
	Przepustowość Threat Protection	600 Mb/s
	Przepustowość NGFW	800 Mb/s
	Funkcje	Zapora sieciowa, bieżąco aktualizowane moduły antywirus, moduły antyspyware i antymalware, VPN IPsec, VPN SSL, ochrona przed włamaniami, kontrola aplikacji, ochrona przed wyciekami informacji, filtrowanie sieci, antyspam.
	Integracja	Integracja i pełne wsparcie wszystkich funkcjonalności z posiadanym przez Zamawiającego Forti Analyzer, integracja z Forti Manager i Forti Explorer.
	Certyfikaty	Produkt musi posiadać certyfikaty: CE, CB
	Wypożyczenie	UTM musi być przystosowany do bezpośredniego montażu w szafie 19" i zawierać kompletny adapter rack tak by umożliwić podłączenie okablowania od przodu
	Gwarancja	12 miesięcy
	Warunki wsparcia	Urządzenie wraz z licencją na moduły antywirusa, ochrony przed atakami, kontroli aplikacji, ochrony przed wyciekami danych. Usługa wsparcia i gwarancji producenta na okres 1 roku
	Wsparcie techniczne	Dostarczany sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

3	Zasilacz awaryjny rack (CPV 30237280-5)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia

	Ilość zamawiana	2 urządzenia
	Typ obudowy	Rack 2U wraz uchwytami montażowymi
	Głębokość urządzenia	Maksymalnie 440 mm
	Moc pozorna	750VA min.
	Moc rzeczywista	500 W min.
	Kształt napięcia wyjściowego	Czysty sinus
	Gniazda wyjściowe	C13 x 4szt.
	Sygnalizacja pracy	Wyświetlacz LCD, dźwiękowa, diody
	Technologia	Line-interactive
	Czas podtrzymania dla 50%	Min. 15 minut
	Wymiana akumulatorów	Wymiana możliwa podczas pracy zasilacza
	Interfejs komunikacyjny	USB, RS-232, LAN
	Test baterii	Automatyczny test baterii
	Zabezpieczenia	Zabezpieczenie przeciążeniowe, przeciwzwarcowe, przeciwprzepięciowe, termiczne, zabezpieczenie przed przeładowaniem
	Dedykowana karta zarządzania	Możliwość doposażenia zasilacza w kartę zarządzania z interfejsem RJ45 pozwalającej na zdalne monitorowanie zasilaczem UPS poprzez sieć, wysyłanie powiadomień o problemach czasie rzeczywistym, planowanie wyłączenia i włączenia, shutdown po sieci
	Sygnalizacja pracy	Wyświetlacz LCD, sygnalizacja dźwiękowa
	Wyposażenie w standardzie	Interfejs RJ45 pozwalający na komunikację i zdalne monitorowanie urządzenia poprzez chmurę
	Certyfikaty produktu	Produkt musi posiadać certyfikaty: CE, EAC

	Produkt spełnia normy	EN/IEC 62040-1:2019/A11:2021
	Deklaracje	RoHS
	Gwarancja	36 miesięcy na zasilacz i 24 miesiące na akumulator
	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

4	Zasilacz awaryjny rack (CPV 30237280-5)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia
	Ilość zamawiana	1 urządzenie
	Typ obudowy	Rack 2U wraz uchwytami montażowymi
	Moc pozorna	2200 VA min.
	Moc rzeczywista	1980 W min.
	Kształt napięcia wyjściowego	Sinusoidalny
	Gniazda	IEC 320 C13 x 8szt.
		IEC 320 C19 x 1szt.
		RJ-45
		USB
	Sygnalizacja pracy	Wyświetlacz LCD, dźwiękowa, diody
	Czas przełączenia	6ms

	zasilania	
	Auto-restart	TAK
	Technologia line-interactive	Line-interactive
	Czas podtrzymania dla 50%	Min. 15 minut
	Interfejs komunikacyjny	RJ-45, USB
	Zabezpieczenia	Przeciążeniowe, przeciwzwarceniowe, przeciwprzepięciowe, termiczne, zabezpieczenie przed przetądowaniem
	Dedykowana karta zarządzania	Karta zarządzania z interfejsem 1xRJ45, dedykowana aplikacja zarządzania (zdalne monitorowanie zasilacza UPS poprzez sieć, wysyłanie powiadomień o problemach czasie rzeczywistym, planowanie wyłączenia i włączenia, shutdown)
	Sygnalizacja pracy	Wyświetlacz LCD, sygnalizacja dźwiękowa
	Certyfikaty produktu	Produkt musi posiadać certyfikaty: CE, EAC
	Produkt spełnia normy	EN/IEC 62040-1:2019/A11:2021
	Deklaracje	RoHS
	Gwarancja	36 miesięcy na zasilacz i 24 miesiące na akumulator
	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

5	Serwer NAS (PVC-48823000-3)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia

Ilość zamawiana	1 urządzenie wraz z kompletem szyn umożliwiającym montaż i wysunięcie z szafy rack
Rodzaj	Serwer NAS typu rack 2U z obsługą minimum 8 dysków
Ilość obsługiwanych dysków	8
Interfejs obsługi dysków	Serial ATA III
Obsługiwane rozmiary dysków	2.5,3.5"
Obsługiwane poziomy RAID	0, 1, 5, 6, 10, 50, 60
Obsługiwane systemy plików	FAT32, HFS+, NTFS, ZFS, exFAT, ext3, ext4
Możliwość obsługi dysków SSD	Dwa porty M.2 PCIe Gen3
Procesor	4 rdzeniowy, 8 wątkowy (minimum), taktowany 2,2GHz (minimum) umożliwiający osiągnięcie wyniku min. 4,500 w teście CPU Mark ze strony www.cpubenchmark.net
Pamięć wewnętrzna	8 GB
Typ pamięci wewnętrznej	DDR4
Maksymalna pamięć operacyjna RAM	64 GB
Ilość wbudowanych portów Ethernet LAN (RJ-45)	2
Gniazda PCI Express x8 (Gen 3.x)	1 (min.)
Porty 10GbE	2 porty RJ45 z obsługą 10GbE, 5GbE, 2,5GbE, 1GbE (dozwolone zastosowanie dodatkowej karty)
Prędkość transferu wbudowanych portów	100,1000,2500 Mbit/s

	LAN	
	Serwer DHCP	Tak
	Obsługa iSCSI	Tak
	Protokoły sieciowe	IPv4, IPv6
	Ilość portów USB 3.2 Gen 2 (3.1 Gen 2) Typu-A	2
	Ilość portów USB 3.2 Gen 2 (3.1 Gen 2) Typu-C	2
	Protokoły zarządzające	SNMP V2/V3
	Obsługa S.M.A.R.T.	Tak
	Wsparcie szyfrowania	256-bit AES, FIPS 140-2, HTTPS, SSH
	Obsługiwane systemy operacyjne Windows	Windows 10, Windows 8, Windows 7, Windows 11
	Obsługiwane systemy operacyjne serwera	Windows Server2016, Windows Server 2019,Windows Server 2022, Windows Server 2025
	Certyfikaty wirtualizacji	Serwer musi posiadać certyfikat potwierdzający prawidłowe współdziałanie z Hyper-V, VMware, Veeam
	Ilość jednostek zasilania	2
	Zarządzanie	Nadzór i zarządzanie oraz pełne wsparcie wszystkich funkcjonalności oferowanych przez platformę zarządzania AMIZcloud funkcjonującą u Zamawiającego
	Certyfikat	CE
	Gwarancja	24 miesiące

	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.
--	---------------------	--

6	Dyski HDD SATA (CPV-30234100-9)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia
	Ilość zamawiana	14 dysków
	Przeznaczenie	Środowisko NAS
	Pojemność HDD	12TB
	Szybkość HDD	7200 RPM
	Rozmiar HDD	3.5"
	Interfejs	Serial ATA III
	Szybkość transmisji interfejsu HDD	6 Gbit/s
	Limit obciążenia pracą	Min. 180 TB/rok
	Średni czas do awarii (MTTF)	Min. 1000000 h
	Kompatybilność	Produkt musi znajdować się na liście dysków kompatybilnych z zaproponowanymi serwerami NAS
	Gwarancja	24 miesiące
	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

7	Oprogramowanie do tworzenia kopii bezpieczeństwa (CPV-48710000-8)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego oprogramowania
	Ilość	Ilość licencji powinna zapewniać backup dla 15 wirtualnych serwerów i 30 fizycznych
	Typ licencji	Licencja wieczysta
	Wymagane funkcjonalności	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
		Rozwiązanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych
		Rozwiązanie musi współpracować z Proxmox VE
		Rozwiązanie zapewnia tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure, AWS S3
		Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiegokolwiek funkcjonalności
		Natywne zapewnia mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
		Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
		Oprogramowanie musi tworzyć integralne archiwa do odzyskania, których nie wymagana jest dodatkowa baza danych z metadanymi
		Oprogramowanie musi wspierać niezmiennosć kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu
		Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania

		Oprogramowanie musi posiadać integracje z systemami typu SIEM
		Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
		Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
		Oprogramowanie musi oferować portal, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, baz danych MS SQL, PostgreSQL
		Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności.
		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.
		Wykorzystywane mechanizmy CBT muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej: VMware, Hyper-V
		Oprogramowanie musi posiadać funkcjonalność modyfikacji obciążenia dostępu zasobów storage dla platform VMware i Hyper-V
		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.
		Oprogramowanie musi posiadać certyfikację VMware na wsparcie funkcjonalności vSAN
		Oprogramowanie musi mieć możliwość generowania retencji
		Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019, 2022, 2025 z systemem pliku ReFS oraz linuxowych XFS
		Rozwiązanie musi mieć możliwość wykorzystania z wbudowanej akceleracji WAN dla realizacji backupów i replikacji.
		Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik

		<p>Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.</p>
		<p>Oprogramowanie musi pozwalać na migrację on-line uruchomionych z pliku backupu maszyn na storage produkcyjny</p>
		<p>Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB, baz danych MS SQL, PostgreSQL bezpośrednio ze skompresowanego pliku backupu i przeniesienie ich on-line na środowisko produkcyjne</p>
		<p>Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków</p>
		<p>Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików</p>
		<p>Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.</p>
		<p>Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux.</p>
		<p>Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM</p>
		<p>Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.</p>
		<p>Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2016 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego, całych baz lub pojedynczych tabeli, widoków oraz procedur.</p>
		<p>Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.</p>
		<p>Oprogramowanie musi 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</p>

		Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych.
		Oprogramowanie musi posiadać swój wbudowany program antywirusowy zoptymalizowany do przeszukiwania kopii backupowych
		Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware
		Oprogramowanie musi posiadać mechanizm wykrywania oznak ataku hakerskiego
		Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa
		Oprogramowanie musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków
		Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością uruchomienia dowolnego skryptu przed odtworzeniem danych
		W środowiskach fizycznych rozwiązanie musi wspierać najnowsze, oficjalne operacyjne systemy Windows w wersjach klienckich oraz serwerowych wykorzystując do wykonania kopii agenta znajdującego się wewnątrz systemu operacyjnego.
		Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, Rocky Linux, AlmaLinux
		Dla maszyn fizycznych rozwiązanie musi wspierać odzyskiwanie całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
		Rozwiązanie musi wspierać backup podłączonych dysków USB
		W środowiskach fizycznych rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
		Kopia zapasowa całej maszyny fizycznej oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
		Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, DAS- zewnętrzne dyski USB, eSATA, NAS - pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)

		Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
		Rozwiązanie musi wspierać kontrolę i dostępność pasma transmisji sieciowej
		Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
		Rozwiązanie musi wspierać technologię BitLocker
		Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
		Rozwiązanie musi wspierać szyfrowanie
		Rozwiązanie dla jednostki fizycznej musi wspierać tworzenie wielu zadań backupowych
		System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
		System musi umożliwiać kategoryzację 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
		System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
		System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualne
		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
		System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Adobe PDF

		System musi mieć możliwość analizowania wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
	Wsparcie techniczne	Dostarczone oprogramowanie objęte aktualizacjami i pomocą techniczną na okres 1 roku bez dodatkowych kosztów.
		Wykonawca musi oferować wsparcie certyfikowanych inżynierów w zakresie konfiguracji i integracji z infrastrukturą IT.
	Wsparcie techniczne	Dostarczone oprogramowanie musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

8	Automatyczny przełącznik zasilania (CPV-30237280-5)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia
	Ilość zamawiana	2 urządzenia
	Opis	Automatyczny przełącznik zasilania o wysokiej dostępności, który zapewnia nadmiarowe zasilanie podłączonego sprzętu za pośrednictwem dwóch wejść, po jednym dla każdego źródła prądu.
	Budowa	Rack 1U (z kompletem uchwytów)
	Napięcie wyjściowe	230V
	Złącza wychodzące	12 x C13
	Złącza wejściowe	2 x C20
	Interfejsy	Ethernet 100/1000 Mb
		USB
	Panel LCD	Informacja o stanie źródeł napięcia
		Informacja o obciążeniu

		Informacja o alarmach
		Informacja o wykorzystywanym aktualnie źródle napięcia
	Funkcjonalności dodatkowe	Dedykowana aplikacja producenta umożliwiająca nadzór, zarządzanie, raporty oraz konfigurację wysyłanych powiadomień o alarmach
	Certyfikat	EN 55022 class A
	Gwarancja	24 miesiące
	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

9	Zakup licencji na system wirtualizacji (CPV-48213000-4)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego oprogramowania
	Ilość zamawiana	Licencja powinna obejmować 64 rdzenie (2 serwery, 2 CPU ,16 core)
	Warunki licencji	VMware vSphere Standard 8 - oprogramowanie objęte roczną subskrypcją, licencjonowane w oparciu o liczbę licencji na rdzeń, gdzie wymagana liczba licencji obejmuje minimum 64 rdzenie
	Opis	Przedmiotem zamówienia jest przedłużenie licencji pozwalających na migrację posiadanego oprogramowania firmy VMware. Zamawiający obecnie posiada wersję Essentials Plus. Zamawiający docelowo oczekuje dostawy wersji VMware vSphere Standard 8
	Wymagane funkcjonalności	VSphere Vmotion - migracja maszyn wirtualnych online bez zakłóceń dla użytkowników lub utraty usługi, eliminując konieczność planowania przestojów aplikacji przy konserwacji serwerów.
		Virtual Volumes - wirtualizacja zewnętrznych pamięci masowych (SAN i NAS) oraz zapewnienie zarządzania nimi, oparte na politykach realizowanych przez vCenter.

		Identity Federation - powiązanie Microsoft Active Directory, Microsoft Active Directory Federation Services (AD FS), Microsoft Entra ID, Okta i PingFederate w celu centralnej autentykacji i wieloskładnikowego uwierzytelniania
		vSphere Replication - możliwość wydajnej replikacji danych maszyn wirtualnych, niezależnie od macierzy, przez LAN lub WAN, oraz upraszcza zarządzanie poprzez umożliwienie replikacji na poziomie maszyny wirtualnej
		vCenter High Availability (vCenter HA) - automatyczny restart maszyn wirtualnych po awarii fizycznej maszyny.
		vCenter Server Appliance Migration - narzędzie do migracji i aktualizacji istniejących wdrożeń Windows vCenter do vCenter Server Appliance w jednym kroku
		Trusted Platform Module Support - obsługa TPM 2.0 dodając ochronę bezpieczeństwa sprzętowego do hipervisora.
		TLS 1.2 i 1.3 - kryptograficzne zabezpieczenia danych
		vSphere Lifecycle Manager - zarządzanie obrazami infrastruktury w celu łatania, aktualizowania lub modernizowania klastrów VMware ESX.
		vCenter Lifecycle Management Service - uproszczenie i automatyzacja procesów konserwacji i zarządzania instancji vCenter
	Typ licencji	Roczna subskrypcja
	Warunki wsparcia	Dostarczone oprogramowanie objęte aktualizacjami i pomocą techniczną na okres 1 roku bez dodatkowych kosztów.
	Wsparcie techniczne	Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

10	Przełącznik zarządzalny (CPV-32420000-3)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia

	Ilość zamawiana	2 urządzenia
	Rodzaj	Zarządzalny przełącznik typu rack L3 28x10G SFP+ i 4x SFP28
	Obudowa	Obudowa typu RACK 19" 1U wraz uchwytami montażowymi
	Model	Model urządzenia w najnowszej wersji dostępnej na rynku polskim
	Wydajność urządzenia	min. 760 Gbps
	VLAN (IEEE 802.1q)	Obsługa aktywnych VLAN min. 64
	IGMP snooping	Tak
	Obsługa ramek Jumbo	Tak
	Ochrona pętli własnej	Tak
	Agregacja portów LACP	Tak
	Kontrola burzowa	Tak
	Kontrola przepływu	Tak
	Izolacja portów	Tak
	Obsługa SNMP	TAK (v1,v2,v3)
	Klient DHCP	Tak
	Zarządzalne warstwy	Zarządzanie L3
	Zarządzanie	Kompatybilny, zarządzalny i oferujący wsparcie wszystkich funkcjonalności z posiadanym przez Zamawiającego kontrolerem systemu UniFi
	Wkładki optyczne SFP28	4 wkładki optyczne 25G kompatybilne z SFP28 MM ze złączami LC (łącznie 8 szt.)
	Wkładki optyczne SFP+	4 wkładki optyczne 10G kompatybilne z SFP+ typ MM ze złączami LC (łącznie 16 szt.)
	Wyświetlacz	Urządzenie wyposażone w wyświetlacz informujący o stanie urządzenia, statusie

		poszczególnych portów, aktualizacji oprogramowania
	Certyfikat	CE
	Gwarancja	24 miesiące
	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

11	Zarządzalny przełącznik (CPV-32420000-3)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia
	Ilość zamawiana	2 urządzenia
	Rodzaj	Zarządzalny przełącznik L3 24xRJ45 10GbE + 2xSFP28
	Obudowa	Obudowa typu RACK 19" 1U wraz z szynami lub uchwytyami montażowymi
	Model	Model urządzenia w najnowszej wersji dostępnej na rynku polskim
	Interfejsy sieciowe	24 x RJ45 10GbE (1000/2500/5000/10 000 Mb/s)
		2 x SFP28 25G
	Zarządzalne warstwy	Zarządzanie L3
	Pojemność przełączania	min.580 Gbps
	VLAN (IEEE 802.1q)	Obsługa aktywnych VLAN min. 64

	IGMP snooping	Tak
	Obsługa ramek Jumbo	Tak
	Ochrona pętli własnej	Tak
	Agregacja portów LACP	Tak
	Kontrola burzowa	Tak
	Kontrola przepływu	Tak
	Izolacja portów	Tak
	Obsługa SNMP	TAK (v1,v2,v3)
	Klient DHCP	Tak
	Funkcje L3	Routing między sieciami VLAN w tym samym przełączniku
		Przełącznik DHCP
		Statyczne routowanie między sieciami lokalnymi
	Zarządzanie	Kompatybilny, zarządzalny i oferujący wsparcie wszystkich funkcjonalności z posiadanym przez Zamawiającego kontrolerem systemu UniFi
	Wkładki optyczne SFP28	2 wkładki optyczne kompatybilne z SFP28 typ MM ze złączami LC (łącznie 4 szt.)
	Wyświetlacz	Urządzenie wyposażone w wyświetlacz informujący o stanie urządzenia, statusie poszczególnych portów, aktualizacji oprogramowania
	Certyfikat	CE
	Gwarancja	24 miesiące
	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

12	Punkt dostępowy (CPV-32420000-3)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia
	Ilość zamawiana	3 urządzenia
	Rodzaje wejść/wyjść	1GbE RJ-45
	Standard	Wi-Fi 6 (802.11 a/b/g/n/ac/ax)
	Zasilanie	PoE+
	Częstotliwość	2,4GHz/5GHz/6GHz
	Moc	Min. 26dBm
	Zabezpieczenie	WPA/WPA-PSK/WPA-PSA Ent./WPA2/WPA3
	Przepustowość w paśmie 2,4GHz	600 Mbps (minimum)
	Przepustowość w paśmie 5GHz	2400 Mbps (minimum)
	Typ	Do montażu wewnętrznego
	BSSID	8 na radio
	VLAN	802.1Q
	Wsparcie dla izolacja ruchu gość	Tak
	Montaż	Ściana, sufit
	Zarządzanie	Kompatybilny, zarządzalny i oferujący wsparcie wszystkich funkcjonalności z posiadanym przez Zamawiającego kontrolerem systemu UniFi
	Certyfikat	CE

	Gwarancja	24 miesiące
	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

13	SERWER (CPV 48820000-2)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia i oprogramowania
	Ilość zamawiana	1 urządzenie
	Model	Model serwera w najnowszej wersji dostępnej na rynku polskim oferowanej przez producenta
	Obudowa	Obudowa rack o wysokości 1U z możliwością instalacji do min.8 dysków 2,5 cala, komplet ramek na dyski, komplet szyn umożliwiających montaż w szafie rack i jego wysunięcie
	Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym i wsparcie TPM 2.0
	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
	Procesor	Jeden procesor 16 rdzeni klasy x86 dedykowany do pracy z zaoferowanym serwerem. Minimum 32 wątków. Minimum 30MB Cache, minimum 2.0GHz umożliwiający osiągnięcie wyniku min. 35800 w teście CPU Mark ze strony www.cpubenchmark.net
	Pamięć RAM	32GB pamięci RAM DDR5 w modułach po minimum 16Gb sztuka. Płyta powinna obsługiwać do 1TB na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych dla pamięci. Zabezpieczenia pamięci: Advanced ECC, Memory Page Retire, Fault Resilient Memory.
	Sloty PCI Express	2 x PCIe 4.0 x 16
	Interfejsy Sieciowe	2 x 10/100/1000 Mbit/s RJ-45
	Karta sieciowa	2 x RJ-45, 10 Gb/s, 10GBase-T (dozwolone zastosowanie dodatkowej karty)

	Dyski twarde	2 dyski 480GB SSD, 4 dyski 960SSD do intensywnego odczytu wymieniany bez wyłączania systemu, kompatybilne z modelem serwera. Dyski muszą być z kieszeniami zainstalowane w serwerze.
	Kontroler RAID	Sprzętowy kontroler dyskowy, 8GB cache, obsługujący 12Gb/s SAS/SATA, podtrzymanie bateryjne, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10
	Wbudowane we/wy	Co najmniej: 2 porty USB 2.0, 1 port USB 3.0
	Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
	Zasilanie	Serwer musi być wyposażony w 2 zasilacze o mocy min. 700W certyfikat 80 PLUS wymieniany bez wyłączania systemu
	Bezpieczeństwo	Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą, możliwość wyłączenia w BIOS funkcji przycisku zasilania
		Możliwość wyłączenia w BIOS funkcji przycisku zasilania
		Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
		Moduł TPM 2.0
		Przedni panel obudowy zdejmowalny, zamykany na kluczyk umożliwiający zakrycie dysków, chroniący dyski przed przypadkowym wyjęciem
	Diagnostyka	Możliwość wyposażenia obudowy w panel LCD umieszczony na froncie, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
	Kontroler zdalnego zarządzania	Zarządzanie niezależne od zainstalowanego na serwerze systemu operacyjnego posiadające dedykowany port RJ-45 Gigabit Ethernet
	Realizowane funkcje przez kartę zdalnego zarządzania	Zdalny dostęp do graficznego interfejsu Web karty zarządzającej
		Monitorowanie, zarządzanie, aktualizowanie, rozwiązywanie problemów i naprawa serwera z dowolnego miejsca -bez użycia agentów. Zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera itp.)
		Szyfrowane połączenie (TLS 1.2) oraz autentykację i autoryzację użytkownika
		Zdalny zrzut ekranu, zapis startu serwera

		Wirtualna konsola z dostępem do myszy i klawiatury
		Integracja z Active Directory
		Wsparcie dla WSMAN (Web Service for Management), SNMP, IPMI2.0, SSH
		Możliwość zdalnego monitorowania w czasie rzeczywistym
		Wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
	Certyfikaty	Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, 2022, 2025 x64
		Serwer musi posiadać deklarację CE.
		Potwierdzona zgodność ISO-9001:2015 oraz ISO-14001
	Licencja Serwerowy system operacyjny	Licencja na serwerowy system operacyjny Windows Server 2025 Standard PL– licencja dobrana tak aby przy oferowanych procesorach umożliwić uruchomienie 2 nowych maszyn wirtualnych (dopuszczalna wersja systemu operacyjnego typu ROK-Reseller Option Kit), lub równoważny Tabela 1.
		Licencja bez ograniczeń czasowych (wieczysta)
	Licencja dostępowa	Licencja dostępowa Windows Server 2025 User CAL dla 40 użytkowników umożliwiającą podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności w ramach Active Directory
		Licencja bez ograniczeń czasowych
		Dopuszcza się dostarczenie licencji dostępowych w paczkach licencji
	Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
	Wsparcie techniczne	Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.
		Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.
	Gwarancja	36 miesięcy w miejscu instalacji
	Warunki gwarancji	Zamawiający wymaga, aby Serwis urządzeń był realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem serwisowym Producenta

		Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień firmware, sterowników nawet w przypadku wygaśnięcia gwarancji serwera
		Dostarczony serwer nie może być w fazie end of life i musi być wyprodukowany na przestrzeni do 12 miesięcy od dnia opublikowania przedmiotowego postępowania.
		Dyski twarde nie podlegają zwrotowi organizacji serwisowej – zostają u Zamawiającego
		Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, strona producenta, na której znajduje się nr telefonu oraz adres email, na który można zgłaszać usterki.
		Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA.
		Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

14	SERWER (CPV 48820000-2)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia i oprogramowania
	Ilość zamawiana	1 urządzenie
	Model	Model serwera w najnowszej wersji dostępnej na rynku polskim oferowanej przez producenta
	Obudowa	Obudowa rack o wysokości 1U z możliwością instalacji do min.8 dysków 2,5 cala, komplet ramek na dyski, komplet szyn umożliwiających montaż w szafie rack i jego wysunięcie
	Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem

		firmowym i wsparcie TPM 2.0
	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
	Procesor	Jeden procesor 16 rdzeni klasy x86 dedykowany do pracy z zaoferowanym serwerem. Minimum 32 wątków. Minimum 30MB Cache, minimum 2.0GHz umożliwiający osiągnięcie wyniku min. 35800 w teście CPU Mark ze strony www.cpubenchmark.net
	Pamięć RAM	32GB pamięci RAM DDR5 w modułach po minimum 16Gb sztuka. Płyta powinna obsługiwać do 1TB na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych dla pamięci. Zabezpieczenia pamięci: Advanced ECC, Memory Page Retire, Fault Resilient Memory.
	Sloty PCI Express	2 x PCIe 4.0 x 16
	Interfejsy Sieciowe	2 x 10/100/1000 Mbit/s RJ-45
	Karta sieciowa	2 x RJ-45, 10 Gb/s, 10GBase-T (dozwolone zastosowanie dodatkowej karty)
	Dyski twarde	2 dyski 480GB SSD, 4 dyski 960SSD do intensywnego odczytu wymieniany bez wyłączania systemu, kompatybilne z modelem serwera. Dyski muszą być z kieszeniami zainstalowane w serwerze.
	Kontroler RAID	Sprzętowy kontroler dyskowy, 8GB cache, obsługujący 12Gb/s SAS/SATA, podtrzymanie bateryjne, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10
	Wbudowane we/wy	Co najmniej: 2 porty USB 2.0, 1 port USB 3.0
	Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
	Zasilanie	Serwer musi być wyposażony w 2 zasilacze o mocy min. 700W certyfikat 80 PLUS wymieniany bez wyłączania systemu
	Bezpieczeństwo	Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą, możliwość wyłączenia w BIOS funkcji przycisku zasilania
		Możliwość wyłączenia w BIOS funkcji przycisku zasilania
		Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
		Moduł TPM 2.0

		Przedni panel obudowy zdejmowalny, zamykany na kluczyk umożliwiający zakrycie dysków, chroniący dyski przed przypadkowym wyjęciem
	Diagnostyka	Możliwość wyposażenia obudowy w panel LCD umieszczony na froncie, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
	Kontroler zdalnego zarządzania	Zarządzanie niezależne od zainstalowanego na serwerze systemu operacyjnego posiadające dedykowany port RJ-45 Gigabit Ethernet
	Realizowane funkcje przez kartę zdalnego zarządzania	Zdalny dostęp do graficznego interfejsu Web karty zarządzającej
		Monitorowanie, zarządzanie, aktualizowanie, rozwiązywanie problemów i naprawa serwera z dowolnego miejsca -bez użycia agentów. Zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera itp.)
		Szyfrowane połączenie (TLS 1.2) oraz autentykacje i autoryzację użytkownika
		Zdalny zrzut ekranu, zapis startu serwera
		Wirtualna konsola z dostępem do myszy i klawiatury
		Integracja z Active Directory
		Wsparcie dla WSMAN (Web Service for Management), SNMP, IPMI2.0, SSH
		Możliwość zdalnego monitorowania w czasie rzeczywistym
		Wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
	Certyfikaty	Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, 2022, 2025 x64
		Serwer musi posiadać deklarację CE.
		Potwierdzona zgodność ISO-9001:2015 oraz ISO-14001
	Licencja Serwerowy system operacyjny	Licencja na serwerowy system operacyjny Windows Server 2025 Standard PL– licencja dobrana tak aby przy oferowanych procesorach umożliwić uruchomienie 2 nowych maszyn wirtualnych (dopuszczalna wersja systemu operacyjnego typu ROK-Reseller Option Kit), lub równoważny Tabela 1.
		Licencja bez ograniczeń czasowych (wieczysta)

	Licencja dostępowa	Licencja dostępowa Windows Server 2025 User CAL dla 20 użytkowników umożliwiającą podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności w ramach Active Directory
		Licencja bez ograniczeń czasowych
		Dopuszcza się dostarczenie licencji dostępowych w paczkach licencji
	Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
	Wsparcie techniczne	Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.
		Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.
	Gwarancja	36 miesięcy w miejscu instalacji
	Warunki gwarancji	Zamawiający wymaga, aby Serwis urządzeń był realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem serwisowym Producenta
		Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień firmware, sterowników nawet w przypadku wygaśnięcia gwarancji serwera
		Dostarczony serwer nie może być w fazie end of life i musi być wyprodukowany na przestrzeni do 12 miesięcy od dnia opublikowania przedmiotowego postępowania.
		Dyski twarde nie podlegają zwrotowi organizacji serwisowej – zostają u Zamawiającego
		Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, strona producenta, na której znajduje się nr telefonu oraz adres email, na który można zgłaszać usterki.
		Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA.
		Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.
--	---------------------	--

15	Serwerowy system operacyjny (CPV-32425000-8)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia i oprogramowania
	Licencja	Microsoft Windows Server 2025 Standard 16 core. Elementy przedmiotu zamówienia posłużą m.in. do modernizacji posiadanego już środowiska wirtualnych serwerów opartych o rozwiązanie Microsoft Windows Server do najnowszej wspieranej przez producenta wersji. Nie dopuszcza się licencji typu ROK
	Typ licencji	Licencja bez ograniczeń czasowych (wieczysta)
	Ilość zamawiana	6 licencji Microsoft Windows Server 2025 Standard 16 core
	Opis	Elementy przedmiotu zamówienia posłużą m.in. do modernizacji posiadanego już przez Zamawiającego środowiska wirtualnych serwerów opartych o rozwiązanie Microsoft Windows Server do najnowszej wspieranej przez producenta wersji.
	Wymagania licencji	Warunki licencjonowania muszą zezwalać na zmianę wersji systemu operacyjnego na niższą z zachowaniem wsparcia technicznego oraz na przeniesienie licencji systemu operacyjnego na inny fizyczny serwer.
		Licencje muszą pochodzić z oficjalnego kanału dystrybucji.
		Dopuszcza się dostarczenie licencji elektronicznych dołączonych do wskazanego przez Zamawiającego istniejącego konta klienta
		Dostarczone licencje muszą być nowe, nieużywane i nieaktywowane wcześniej na innym urządzeniu.
	Wymagania techniczne	Możliwość pracy w roli klienta domeny Microsoft Active Directory

		<p>Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2025, 2022</p>
		<p>Możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP</p>
		<p>Zarządzanie komputerami poprzez Zasady Grup (GPO) Active Directory MS Windows (posiadaną przez Zamawiającego), Windows Management Instrumentation.</p>
		<p>Możliwość uruchomienia roli serwera DNS</p>
		<p>Możliwość uruchomienia roli klienta i serwera czasu (NTP)</p>
		<p>Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory</p>
		<p>Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory</p>
		<p>Możliwość uruchomienia roli serwera stron WWW</p>
		<p>Obsługa funkcjonalności szyfrowania dysków</p>
		<p>Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</p>
		<p>Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET</p>
		<p>Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych</p>
		<p>Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</p>
		<p>Wbudowany mechanizm wirtualizacji (hypervisor) umożliwiający uruchamianie wirtualnych systemów w ramach zasobów sprzętowych serwera</p>
		<p>W ramach licencji zawarte prawo do pobierania poprawek systemu operacyjnego</p>
		<p>Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania, nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów.</p>

		Możliwość instalacji w środowiskach wirtualizacyjnych VMware, Proxmox, Hyper-V
		Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
		Wszystkie w/w funkcjonalności nie mogą być realizowane przy zastosowaniu wszelkiego rodzaju emulacji i wirtualizacji
	Licencja dostępowa	Licencja dostępowa Microsoft Windows Server 2025 User CAL dla 60 użytkowników. Umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych zasobów serwera Microsoft Windows Server 2025,2022 i funkcjonalności w ramach Active Directory
		Dopuszcza się dostarczenie licencji dostępowych w paczkach licencji
	Wsparcie techniczne	Dostarczone licencje muszą pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

16	Serwer NAS (PVC-48823000-3)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia.
	Ilość zamawiana	1 urządzenie wraz z kompletem szyn umożliwiających montaż i wysunięcie z szafy rack
	Rodzaj	Serwer NAS typu rack z obsługą 30 dysków 2U
	Ilość obsługiwanych dysków	30
	Interfejs obsługi dysków	Serial ATA III
	Obsługiwane rozmiary dysków	2.5,3.5"
	Obsługiwane poziomy	0, 1, 5, 6, 10, 50, 60

	raid	
	Obsługiwane systemy plików	FAT32, HFS+, NTFS, ZFS, exFAT, ext3, ext4
	Obsługa przyspieszenia pamięci podręcznej SSD	Tak
	Możliwość obsługi dysków SSD	TAK
	Procesor	6 rdzeniowy, 12 wątkowy (minimum), taktowany do 5,1GHz (minimum) umożliwiający osiągnięcie wyniku min. 34000 w teście CPU Mark ze strony www.cpubenchmark.net
	Pamięć wewnętrzna zainstalowana	32 GB
	Typ pamięci wewnętrznej	DDR5
	Maksymalna pamięć operacyjna RAM	128 GB
	Ilość gniazd pamięci	4 x UIDIMM DDR5
	Ilość wbudowanych portów Ethernet LAN (RJ-45)	2 (2,5G/1G)
	Ilość wbudowanych portów 10GbE	2x 10GbE (10G/5G/2,5G/1G)
	Ilość portów 25GbE	2x SFP28 (dozwolone zastosowanie dodatkowej karty)
	Wsparcie wake on LAN (WOL)	Tak
	Gniazda PCIe	3
	Typ PCIe	1 x Gen 4 x 4
		1 x Gen 4 x 8 or Gen 4 x 4

		1 x Gen4 x 4
	Serwer DHCP	Tak
	Obsługa iSCSI	Tak
	Protokoły sieciowe	IPv4, IPv6
	Ilość portów USB 3.2 Gen 2 (3.1 Gen 2) Typu-A	2
	Protokoły zarządzające	SNMP V2/V3
	Obsługa S.M.A.R.T.	Tak
	Wsparcie szyfrowania	256-bit AES, FIPS 140-2, HTTPS, SSH
	Obsługiwane systemy operacyjne Windows	Windows 10, Windows 8, Windows 7, Windows 11
	Obsługiwane systemy operacyjne serwera	Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025
	Ilość jednostek zasilania	2
	Kompatybilność	Serwer musi być posiadać certyfikowane wsparcie platform wirtualizacyjnych: VMware oraz Microsoft Hyper-V, oraz oprogramowania Veeam Backup
	Wypożyczenie	2 wkładki światłowodowe SFP28-LC 25Gbps
	Zarządzanie	Nadzór i zarządzanie przez platformę zarządzania AMIZcloud funkcjonującą u Zamawiającego
	Certyfikat	CE
	Gwarancja	24 miesiące
	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

17	Zarządzalny przełącznik PoE (CPV- 32420000-3)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia.
	Ilość zamawiana	2 urządzenia
	Rodzaj	Zarządzalny przełącznik PoE 24x1G +2 SFP 10G typu rack
	Obudowa	Obudowa typu RACK 19" 1U wraz z szynami lub uchwytyami montażowymi
	Model	Model urządzenia w najnowszej wersji dostępnej na rynku polskim
	Interfejsy sieciowe dostępne od frontu urządzenia	24 x interfejs Ethernet 10/100/1000BaseT(RJ-45) + 2xSFP 10GbE
	Ilość portów PoE	Min. 16x portów PoE+ / 8x portów PoE++
	Budżet PoE	400W
	Wydajność przełączania	88 Gb/s
	VLAN (IEEE 802.1q)	Obsługa aktywnych VLAN min. 64
	IGMP snooping	Tak
	Obsługa ramek Jumbo	Tak
	Ochrona pętli własnej	Tak
	Agregacja portów LACP	Tak
	Kontrola burzowa	Tak
	Kontrola przepływu	Tak
	Izolacja portów	Tak

	Obsługa SNMP	TAK (v1,v2,v3)
	Klient DHCP	Tak
	Zarządzanie	Kompatybilny i zarządzalny z istniejącym u Zamawiającego kontrolerem systemu UniFi
	Wypożyczenie	2 wkładki światłowodowe SFP+ RJ45 1/2.5/5/10 GbE (łącznie 4 szt.)
	Chłodzenie	Bez wentylatora
	Wyświetlacz	Wyświetlacz przedstawiający aktualny status portów urządzenia, adresy IP, alarmy
	Certyfikaty	CE
	Gwarancja	24 miesiące
	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

18	Sprzętowy kontroler nadzoru urządzeń sieciowych (CPV-32420000-3)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia.
	Ilość zamawiana	1 urządzenie
	Rodzaj	Sieciowy kontroler sprzętowy
	Wbudowany dysk	1TB SSD
	Pamięć	2GB RAM
	Zasilanie	PoE (IEEE 802.3af)
	Interfejs sieciowy	1GbE RJ45

	Zarządzanie	Pełne zarządzanie i kompatybilność z istniejącą infrastrukturą sieciową zbudowaną w oparciu o urządzenia UniFi. Zapewnia weryfikację bieżącego stanu urządzeń ich konfigurację oraz zbieranie logów. Integracja z aplikacjami UniFi
	Certyfikaty	CE
	Gwarancja	24 miesiące
	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

19	ZASILACZ AWARYJNY (CPV 30237280-5)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia.
	Ilość zamawiana	10 urządzeń
	Rodzaj	Zasilacz awaryjny UPS stanowiskowy
	Moc pozorna	950 VA
	Moc skuteczna	520W
	Kształt napięcia wyjściowego	Aproksymacja sinusoidy
	Czas podtrzymania dla 50%	5 min (minimum)
	Czas przełączenia	6 ms
	Typ gniazd wyjściowych	4 x Typ E (FR)
	Porty dodatkowe	RJ-45 (in/out)

	Port komunikacji	1 x USB (B)
	Funkcjonalność	Oprogramowanie do samoczynnego i bezpiecznego zamykania systemu oraz funkcji monitoringu i konfiguracji UPS dla Windows 10, Windows 11
	Certyfikaty produktu	Produkt musi posiadać certyfikaty: CE, EN62040-1
	Deklaracje	RoHS
	Gwarancja	24 miesiące
	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

20	Zarządzalny przełącznik (CPV- 32420000-3)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia.
	Ilość zamawiana	3 urządzenia
	Rodzaj	Zarządzalny przełącznik typu rack PoE 16x1GbE +2 SFP
	Obudowa	Obudowa typu RACK 19" 1U wraz z szynami lub uchwytyami montażowymi
	Model	Model urządzenia w najnowszej wersji dostępnej na rynku polskim
	Interfejsy sieciowe dostępne od frontu urządzenia	16 x interfejs Ethernet 10/100/1000BaseT(RJ-45) + 2xSFP
	Ilość portów PoE	Min. 8x portów PoE+ 802.3af/at
	Budżet PoE	40W
	Wydajność urządzenia	Min. 36 Gbps
	VLAN (IEEE 802.1q)	Obsługa aktywnych VLAN min. 64

	IGMP snooping	Tak
	Obsługa ramek Jumbo	Tak
	Ochrona pętli własnej	Tak
	Agregacja portów LACP	Tak
	Kontrola burzowa	Tak
	Kontrola przepływu	Tak
	Izolacja portów	Tak
	Obsługa SNMP	TAK (v1,v2,v3)
	Klient DHCP	Tak
	Zarządzanie	Dostarczony switch musi być kompatybilny i zarządzalny z istniejącym kontrolerem systemu UniFi
	Chłodzenie	Bez wentylatora
	Certyfikaty	CE
	Gwarancja	24 miesiące
	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

21	Punkt dostępowy (CPV- 32420000-3)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego urządzenia.
	Ilość zamawiana	6 urządzenia

	Rodzaje wejść/wyjść	1GbE RJ-45
	Standard	Wi-Fi 5 (802.11 a/b/g/n/ac/ax)
	Zasilanie	PoE+
	Częstotliwość	2,4GHz/5Ghz
	Moc	23dBm min.
	Zabezpieczenie	WPA/WPA-PSK/WPA-PSA Ent./WPA2/WPA3
	Przepustowość w paśmie 2,4GHz	570 Mbps min.
	Przepustowość w paśmie 5GHz	2400 Mbps min.
	Typ	Do montażu wewnątrz
	BSSID	8 na radio
	VLAN	802.1Q
	Wsparcie dla izolacja ruchu gość	Tak
	Montaż	Ściana, sufit (w zestawie)
	Zarządzanie	Kompatybilny i zarządzalny z istniejącym kontrolerem systemu UniFi
	Certyfikaty	CE
	Gwarancja	24 miesiące
	Wsparcie techniczne	Dostarczony sprzęt musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

22	Klucz sprzętowy	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanej licencji
	Ilość zamawiana	4 urządzenia
	Interfejs	USB 2.0
		Wbudowany czytnik linii papilarnych
	Zgodność z przepisami i regulacjami dotyczącymi prywatności	RODO, BIPA i CCPA
	Bezpieczeństwo	Dane linii papilarnych są izolowane i zabezpieczane w czujniku a przekazywany jest tylko zaszyfrowany wynik dopasowania
	Obsługa	Windows Hello i Windows Hello for Business
	Gwarancja	24 miesiące

Zamówienie część 2

1	Oprogramowanie antywirusowe (CPV-48760000-3)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego oprogramowania
	Ilość zamawiana	licencja dla 90 urządzeń
	Opis	Przedmiotem zamówienia jest przedłużenie oraz migracja licencji na posiadane oprogramowanie antywirusowe firmy ESET. Zamawiający obecnie posiada ESET PROTECT Advanced. Zamawiający docelowo oczekuje dostawy wersji ESET PROTECT

		Enterprise – 90 stanowisk ważnych do 30.06.2026 r
	Oprogramowanie powinno zawierać następujące moduły funkcjonalne	Moduł: antywirus, firewall, szyfrowanie dysków, sandbox, EDR, konsola lokalna oraz chmurowa
	Wsparcie techniczne	Dostarczone oprogramowanie musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

Zamówienie część 3

1	Przedłużenie i rozszerzenie licencji wsparcia na oprogramowanie monitorowania i zarządzania siecią (CPV-48210000-3)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego oprogramowania
	Ilość zamawiana	Przedłużenie licencji dla 55 urządzeń oraz 35 nowych licencji
	Opis	Przedłużenie posiadanej przez Zamawiającego licencji nVision na 55 urządzeń oraz dodatkowo 35 nowych licencji EDU wraz ze wsparciem i gwarancją producenta na okres 1 roku.
	Licencja	Licencja wieczysta na oprogramowanie Axence nVision
	Licencja musi zawierać moduły	Network
		Inventory
		Users
		Helpdesk
		DataGuard

		SmartTime
	Wsparcie techniczne	Dostarczone oprogramowanie objęte aktualizacjami i pomocą techniczną na okres 1 roku bez dodatkowych kosztów.

Zamówienie część 4

1	Oprogramowania do zarządzania dostępem uprzywilejowanym (CPV-48780000-9)	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego oprogramowania
	Ilość zamawiana	licencja dla 5 jednoczesnych dostępów
	Warunki licencji	Licencja wieczysta dla co najmniej 5 użytkowników (jednoczesny dostęp) z rocznym serwisem, dostępem do aktualizacji i wsparciem technicznym
		Brak limitów na ilość chronionych zasobów infrastruktury informatycznej.
	Zakres licencji	Licencja musi obejmować funkcjonalności:
		Ochrona i zarządzanie kontami uprzywilejowanymi
		Rejestrowanie i archiwizacja zdalnych sesji
		Zarządzanie i monitorowanie sesji uprzywilejowanych
		Ochrona kluczy SSH
		Gwarancja skalowalności rozwiązania w przypadku dodawania nowych zasobów oraz nowych usług
		Raportowanie wykorzystania kont uprzywilejowanych
	Wymagania	System ma zabezpieczać dostęp do maszyn wirtualnych i fizycznych, aplikacji, baz danych, ruterów, przełączników oraz pozostałej infrastruktury sieci aktywnej
		Dostarczony system musi być przygotowany do implementacji w istniejącej

		infrastrukturze zamawiającego VMware w formie zamkniętej platformy wirtualnej.
		Do prawidłowego działania wszystkich dostępnych funkcjonalności wymagane jest posiadanie tylko jednej maszyny wirtualnej w ramach której zainstalowana jest całość oprogramowania
		Rozwiązanie nie może wymagać instalacji dodatkowych komponentów w formie odrębnych maszyn wirtualnych lub fizycznych
		System musi opierać się na rozwiązaniu bezagentowym eliminując konieczność jego instalacji na zasobie do którego nawiązywane jest połączenie.
		Rozwiązanie musi oferować funkcjonalność pracy w klastrze HA w konfiguracji active-active ¹⁹
	Funkcje zarządzania	Możliwość zarządzania w ramach kont domenowych MS Active Directory
		Zarządzanie użytkownikami w systemach Windows, Linux
		zarządzanie kontami lokalnymi VMware ESX/ESXi
		Zarządzanie kontami baz danych: Microsoft SQL, MySQL, PostgreSQL
		Zarządzanie i monitorowanie kontrolerów zdalnego dostępu do serwerów iDRAC, iLO
		Zarządzanie kontami na urządzeniach: Dell, Huawei, Fortinet, Cisco
		zarządzanie kontami aplikacji webowych: facebook, Google, Instagram, AWS
		Zarządzanie kontami w systemach zewnętrznych obsługujących protokoły: SSH, RDP VNC, TELNET, HTTP/HTTPS
		System musi wspierać protokoły dla sesji: iLDAP, LDAPS, MySQL, PostgreSQL, SQL Server Windows SMB, Windows RPS
		System musi umożliwiać transparentne połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego
		Wymaga się aby system wspierał zmiany wartości hasła na systemie docelowym zgodnie z ustawioną polityką m.in.:
		- możliwość zdefiniowania wymagań na: długość hasła, znaki w hasle (małe i duże litery, cyfry, znaki specjalne)

		- generowanie unikalnego hasła dla konta systemów docelowych
		- wymuszanie automatycznej zmiany hasła po jego podglądzie
		System musi umożliwiać budowanie polityk kontroli dostępu w oparciu o przynależności do grup AD/LDAP
		System musi umożliwiać budowanie polityk kontroli dostępu wymuszającej:
		- konieczność akceptacji rozpoczęcia sesji przez innego administratora
		- zakresu godzin, dni oraz dat kiedy użytkownik systemu będzie miał dostęp do poświadczeń
		- podanie powodu rozpoczęcia sesji
	Funkcjonalności systemu	System musi wspierać dostęp użytkowników do docelowego systemu narzędziami typu: przeglądarka internetowa, klient RDP, klient SSH, klient serwerów bazodanowych
		System musi umożliwiać wdrożenie uwierzytelniania dwuskładnikowego
		System musi wspierać istniejące mechanizmy uwierzytelniania: LDAP, RADIUS, Tacacs Active Directory, OpenID, SAML
		System musi wspierać integrację z rozwiązaniami dwuskładnikowego uwierzytelnienia takimi jak Google Authenticator i Microsoft Authenticator.
		System powinien posiadać zdolność do utworzenia poświadczeń które będą aktywne tylko na czas trwania konkretnej sesji.
		System musi umożliwiać usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych oraz użytkowników zewnętrznych, rejestrując obsługiwane sesje, oraz obsługując minimum następujące protokoły: SSH, RDP,VNC, TELNET, HTTP/HTTPS
		System musi obsługiwać ograniczanie dostępu do systemów docelowych oraz tworzenie białych i czarnych list poleceń wykonywanych w systemie docelowym.
		System musi być wyposażony w funkcjonalność weryfikacji poleceń pozwalającą na podjęcie akcji, zablokuj polecenie i rozłącz sesję po wykryciu polecenia a także automatyczne umieszczenie na liście blokowanych użytkowników użytkownika, który próbował wykonać blokowane polecenie
	Funkcje logowania i	System musi tworzyć logi dla wszystkich zdarzeń systemowych

	raportowania	
		System musi umożliwiać weryfikację kont użytkowników, którzy realizowali logowanie do stacji/serwera.
		System musi umożliwiać raportowanie wszystkich logowań do systemu.
		Rozwiązanie musi umożliwiać raportowanie wszystkich zmian wprowadzonych przez administratorów.
		System musi umożliwiać raportowanie oparte na analizie m.in. nietypowego źródła ruchu , czasie i długości połączenia do systemu docelowego.
		Rozwiązanie powinno być w stanie zobrazować aktualny stan bezpieczeństwa aktywnych oraz historycznych sesji do systemów zdalnych.
		System musi umożliwiać podgląd zestawionej sesji w czasie rzeczywistym.
		System musi umożliwiać przerwanie lub zawieszenie trwającej zarówno pojedynczej sesji jak i wszystkich sesji, oraz całkowite zablokowanie dostępu.
		System musi obsługiwać monitorowanie i ochronę kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego, do różnych systemów poprzez wiele lub jedno konto uprzywilejowane.
	Rejestracja sesji	Uruchomienie funkcji nagrywanie sesji nie może mieć żadnego wpływu na wydajność systemu docelowego
		System musi rejestrować znaki wprowadzone z klawiatury przez użytkownika co najmniej dla sesji SSH i RDP oraz umożliwiać szybkie przeszukiwanie zapisanych danych pod kątem występowania wskazanych słów kluczowych
		System musi umożliwiać odtworzenie i pobranie zarejestrowanych nagrań sesji.
		W zakresie nagrywania sesji rozwiązanie musi umożliwiać konfigurację następujących parametrów:
		- długości przechowywania nagrań
		- ilości klatek na sekundę
		- jakości pojedynczej klatki
		- formatu zapisu pojedynczej klatki: jpg lub png

		System musi umożliwiać zbudowanie oddzielnego zestawu reguł w oparciu o:
		- ustaloną politykę dostępową
		- urządzenie docelowe
		- adresu źródłowego
		- poświadczenie
	Wsparcie techniczne	Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

Zamówienie część 5

1	Oprogramowanie ochrony poczty typu Email Gateway	
	Nazwa	W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego oprogramowania
	Ilość zamawiana	40 kont pocztowych objętych roczną subskrypcją
	Opis	Oprogramowanie ochrony poczty elektronicznej z wykorzystaniem odrębnego serwera pośredniczącego dla wielu domen
	Wymagane funkcjonalności systemu	Zarządzanie użytkownikami i grupami oraz ich synchronizacja z Active Directory
		Uwierzytelnianie wspierające SPF, DKIM i DMARC
		System przenosi wiadomości do kwarantanny jeśli wykryto nieprawidłowości w DMARC
		System przenosi wiadomości do kwarantanny jeśli wykryto nieprawidłowości w SPF

		Rozwiązanie zapewniać ochronę przed malware na podstawie sygnatur, analizy behawioralnej oraz heurystycznej
		Blokowanie nadawcy na podstawie geolokalizacji
		Monitorowanie i rejestracja prób dostępu do skrzynek pocztowych
		Rozwiązanie musi wspierać analizę reputacji domen i adresów IP
		System domyślnie musi wspierać komunikację TLS i wykluczać serwery pocztowe które jej nie obsługują.
		System powinien posiadać wiele silników i mechanizmów wykrywania spamu i ataków
		Funkcja antymalware która wykrywa złośliwe oprogramowanie na podstawie zawartości lub zachowania
		Rozwiązanie powinno udostępniać możliwość wyodrębnienia kwarantanny całej firmy dla pojedynczego użytkownika pod kątem spamu i wirusów.
		Funkcja czarnej i białej listy dla pojedynczego użytkownika i całej firmy.
		Funkcje analizy pozwalające zidentyfikować prawdziwego nadawcę wiadomości tak by można wykryć ataki podszywania się
		System musi wykrywać malware w VBA, makrach i dokumentach Microsoft Office]
		System musi wykrywać czy wiadomości są zaszyfrowane lub podpisane cyfrowo
		System musi sprawdzać czy nagłówki są spreparowane aby przypominały prawidłową nazwę domeny
		System musi zapewniać szczegółowy audyt wiadomości obejmujący w szczególności dokładną informację o dostarczeniu wiadomości bądź powodów jej odrzucenia
		System potrafi porównywać domenę nadawcy z prawdziwymi nazwami domen, aby zidentyfikować domeny różniące się od rzeczywistej nazwy domeny jednym lub dwoma znakami.
		System musi wykrywać archiwa zabezpieczone hasłem
		System musi posiadać możliwość określenia maksymalnej ilości wiadomości wysłanych przez użytkownika.

		System musi posiadać możliwość odrzucania wiadomości większych niż ustalona wartość.
		System musi wykrywać i odrzucać wiadomości w których występują określone słowa
		System musi wspierać filtrowanie wiadomości w oparciu o nazwę załącznika
		Monitorowanie limitu wysyłania - mechanizm zapobiegający umieszczeniu domeny na czarnej liście.
		Ochrona w czasie kliknięcia obejmująca działania:
		- sprawdzenie reputacji
		- blokowanie przekierowania na inny adres
		- skanowanie łączy w momencie dostarczenia wiadomości
		- skanowanie w momencie kliknięcia
		System umożliwia budowanie indywidualnych polityk obejmujących kontrolę dostarczania wiadomości na podstawie m.in..
		- nagłówka
		- załącznika
		- słów kluczowych
		- rozmiaru wiadomości
		- czasu
		- źródła wiadomości
		- miejsca docelowego
		- wyniku kontroli antyspamowej
		System musi posiadać kreator raportów z opcją eksportu i zawierających definiowane pola i kryteria odejmujące m.in..
		- czas

		- temat
		- adres nadawcy
		- IP nadawcy
		- odbiorca
		- kierunek wiadomości
		- nazwa użytej reguły
		- akcja końcowa filtrowania wiadomości
		Rozwiązanie umożliwia szczegółowe zobrazowanie przepływu poczty w tym wyzwalanych reguł i podjętych działań.
		System umożliwia przechowywanie i automatyczną archiwizację logów
		Rozwiązanie musi być wyposażone funkcje budowy harmonogramów realizujących kreślone raporty.
		System umożliwia przysyłanie raportów po wykryciu wystąpienia reguł alarmowych.
	Wsparcie techniczne	Dostarczona licencja musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie techniczne producenta na terenie Polski.

Zamówienie część 6

1	Dostarczenie i wdrożenie aplikacji zapewniającej jednolity system logowania do aplikacji dziedzinowych z centralnym menadżerem haseł (CPV-48780000-9)	
	Opis	Przedmiotem zamówienia jest dostarczenie i wdrożenie aplikacji zapewniającej jednolity system logowania do aplikacji dziedzinowych oraz EZD. Aplikacja musi ewidencjonować operację logowania użytkowników do systemów dziedzinowych oraz zapewnić pełną rozliczalność operacji administracyjnych, w tym zmianę parametrów i ustawień programowania.

	Ilość	Wszyscy użytkownicy aplikacji dziedzinowych (brak limitu ilości użytkowników w organizacji)
	Wymagania	System musi posiadać panel administracyjny z możliwością instalacji w sieci odseparowanej od użytkowników systemu
		System musi posiadać wydzielony moduł uwierzytelniania
		System musi przechowywać odrębną tożsamość użytkowników, niezależną od tożsamości bazodanowej aplikacji dziedzinowych
		Rozwiązanie musi pozwalać na definicję wzorców na podstawie, których tworzeni są użytkownicy
		System musi posiadać zunifikowane zarządzanie danymi identyfikacyjnymi użytkowników - takie jak hasła, loginy, uprawnienia do aplikacji
		System musi pozwalać na grupowe wprowadzanie użytkowników z danych zewnętrznych na podstawie np. pliku xlsx czy poprzez integrację z dziedzinowym systemem kadrowym
	Definicja kont użytkowników:	Wskazanie czasu ważności konta dla użytkownika
		Możliwość zdefiniowania dolnej ilości profili i haseł
		Wymuszanie zmiany hasła przy pierwszym (kolejnym) zalogowaniu do systemu
		Możliwość ustawienia losowego hasła z powiadomieniem użytkownika przez email
		Wymuszanie zmiany hasła zgodnie ze zdefiniowaną częstotliwością
		Możliwość zdefiniowania ograniczenia ilości zmian hasła przez użytkownika w okresie czasu
		Blokowanie i odblokowywanie konta użytkownika
		Możliwość określenia liczby nieudanych prób logowania, po których użytkownik zostanie zablokowany
		Wyszukiwanie użytkowników
	Uwierzytelnianie	System musi wspierać uwierzytelnianie poświadczeniami domenowymi - integracja Active Directory

		System musi wspierać protokół uwierzytelniania OIDC
		Rozwiązanie musi obsługiwać jednokrotne logowanie do wielu aplikacji - SSO
		Obsługa uwierzytelniania poświadczeniami Windows
		Uwierzytelnianie oparte o tokeny
	Funkcje obsługi dostępu w ramach organizacji	Możliwość obsługi centralnej struktury organizacyjnej z pełną historią zmian i możliwością sprawdzania stanu na dany dzień
		Możliwość importu danych struktury organizacyjnej z Microsoft Active Directory
		System musi oferować możliwość sterowania dostępem do instancji aplikacji na poziomie organizacji
		System musi oferować możliwość definicji ram czasowych dla przypisania użytkownika do aplikacji
		System musi obsługiwać listy dostępnych instancji aplikacji
		Rozwiązanie musi wspierać identyfikację instancji aplikacji poprzez identyfikatory, dozwolone adresy URL i obsługiwaną metodę uwierzytelniania
		System zapewnia uwierzytelnianie instancji modułów aplikacji poprzez dedykowane identyfikatory i klucze
	Historia operacji użytkownika	System musi monitorować następujące operacje związane z aktywnością użytkownika: autoryzacja, wylogowanie, aktywność użytkownika, uwierzytelnienie, błąd uwierzytelnienia, błąd autoryzacji, zablokowanie użytkownika, blokowanie z powodu osiągnięcia limitu nieudanych prób logowania, odblokowanie użytkownika, autoryzacja zmiany hasła
	Historia operacji administratora	System musi monitorować następujące operacje związane z aktywnością administratora:
		- dodanie, edycja, usunięcie użytkownika
		- nadanie użytkownikowi roli w organizacji
		- przypisanie użytkownika do grupy użytkowników
		- usunięcie użytkownika do grupy użytkowników

		- dodanie, edycja, usunięcie komórki organizacyjnej
		- przypisanie użytkownika do komórki organizacyjnej
		- usunięcie użytkownika z komórki organizacyjnej
		- usunięcie przypisania aplikacji do organizacji
		- zmiana loginu lub hasła użytkownika
		- zablokowanie użytkownika
		- odblokowanie użytkownika
		- usunięcie komórki organizacyjnej
		- zmiana ustawień globalnych
	Monitorowanie i raportowanie	System musi oferować możliwość szybkiego bezpiecznego wylogowania użytkowników z aplikacji dziedzinowych przez administratora
		System musi oferować szybkie blokowanie dostępu użytkowników do aplikacji dziedzinowych przez administratora
		System musi pozwalać na szybką weryfikację stanu kluczowych usług systemów dziedzinowych
		System musi pozwalać na szybką weryfikację kopii zapasowych udostępnionych systemów dziedzinowych
		System musi posiadać funkcjonalność wysyłania wiadomości i powiadomień do użytkowników
	Typ licencji	Licencja bezterminowa
	Wsparcie techniczne	Dostawca powinien zapewnić przeszkolenie personelu odpowiedzialnego za zarządzanie systemem oraz udzielić wsparcia technicznego dla wdrożonego rozwiązania na okres do 30.06.2026 r.

Tabela 1 – Część 1. Parametry równoważności w stosunku do pozycji - serwer, element "Licencja serwerowy system operacyjny"

Specyfikacja funkcjonalności	
W ofercie wymagane jest podanie pełnej nazwy handlowej (producent, symbol) oferowanego oprogramowania	
W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2025 , Zamawiający wymaga dostarczenia odpowiedniej ilości licencji dla serwera fizycznego oraz serwerów wirtualnych, oraz instalację i migrację obecnego środowiska. Zamawiający wymaga aby produkt równoważny spełniał niżej wymienione wymagania:	
Współpraca z procesorami o architekturze x86 – 64bit	
Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.	
Możliwość budowania klastrów składających się z 64 węzłów.	
Licencja/licencje muszą obsługiwać serwer fizyczny wyposażony w zaproponowane procesory / fizyczne rdzenie.	
Praca w roli klienta domeny Microsoft Active Directory.	
Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2025.	
Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.	
Możliwość uruchomienia roli klienta i serwera czasu (NTP).	
Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.	
Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.	
Możliwość uruchomienia roli serwera stron WWW.	
W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.	

W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.	
Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).	
Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.	
Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.	
Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).	
Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość	
Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.	
Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET	
Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.	
Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.	
Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.	
Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.	
Mechanizmy logowania w oparciu o: a) login i hasło, a) karty z certyfikatami (smartcard), b) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).	

Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: a) określonych grup użytkowników, b) zastosowanej klasyfikacji danych, c) centralnych polityk dostępu w sieci, d) centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.	
Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).	
Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.	
Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.	
Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).	
Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.	
Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:	
a) podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.	
b) usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: • podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, • ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, • odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, • bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.,	
c) zdalna dystrybucja oprogramowania na stacje robocze	
d) praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników	

e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające: <ul style="list-style-type: none"> • Dystrybucję certyfikatów poprzez http, • Konsolidację CA dla wielu lasów domeny, • Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, • Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 	
f) szyfrowanie plików i folderów	
g) szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec)	
h) szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi	
i) możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów	
j) serwis udostępniania stron WWW	
k) wsparcie dla protokołu IP w wersji 6 (IPv6)	
l) wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows	
m) wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera)	
n) możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.	
o) możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.	
p) mechanizmy wirtualizacji mające wsparcie dla: <ul style="list-style-type: none"> • dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, • obsługi ramek typu jumbo frames dla maszyn wirtualnych. • obsługi 4-KB sektorów dysków, • nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, • możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego. 	
q) możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.	

na Rozwój Cyfrowy

r) wsparcie dla rozwiązania Kubernetes.	
s) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.	
t) wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).	
u) mechanizmy deduplikacji i kompresji na wolumenach.	
v) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.	
w) mechanizm konfiguracji połączenia VPN do platformy Azure.	
x) wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.	
y) mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.	
z) możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).	