Załącznik nr 1 do SWZ – Opis Przedmiotu zamówienia

1. Urządzenie do przechowywania i udostępniania danych – NAS

Producent: …….

Model: ……..

Ilość: 1 szt.

Nazwa	Wymagane parametry techniczne
Procesor	Zainstalowany jeden procesor min. 4-rdzeniowy klasy x86, min. 3,35GHz, dedykowany do pracy z zaoferowanym urządzeniem
Pamięć	Min. 32 GB Korekcja ECC
Pamięć masowa	Kieszeń/kieszenie na dyski: min. 12 szt. Obsługiwane dyski twarde: - 3.5" SATA HDD - 2.5" SATA SSD Dysk z możliwością wymiany podczas pracy (hot-swap)
Zainstalowane dyski	Zainstalowane min. 12 szt. dysków kompatybilnych z urządzeniem o parametrach: - pojemność: min. 6TB - Interfejs: SATA min. 6 Gb/s - prędkość obrotowa min. 5400 obr/min. W ofercie podać producenta i model dysków
Porty zewnętrzne	Port LAN RJ-45 1GbE: min. 2 szt. Port LAN RJ-45 10GbE: min. 1 szt. Port LAN SFP+ 10GbE: min. 2 szt. Port USB 3.x: min. 2 szt.
Zasilanie	Zasilanie redundantne min. 350W
Inne	Wykonawca dostarczy zestaw szyn do montażu w szafie rack oraz 2 szt. pasywnego przewodu dwuosiowego o długości min. 1 metra i konektory SFP+(10Gbps) po obydwu stronach przewodu
Gwarancja	Gwarancja producenta min. 36 miesięcy
Termin realizacji	Dostawa do 90 dni od dnia podpisania umowy

2. Przełączniki sieciowe zarządzalne wraz z niezbędnym wyposażeniem oraz kontrolerem sprzętowym Ilość: 1 kpl.

Parametr	Charakterystyka (wymagania minimalne)
Przełącznik typ 1	Cechy sprzętowe: • Urządzenie musi być wyposażone w min. 16 portów SFP+ • Porty SFP+ muszą obsługiwać wkładki o prędkości zarówno 1Gbps jak i 10Gbps • Urządzenie musi być wyposażone w port konsoli umożliwiający zarządzanie urządzeniem z poziomu linii komend • Dopuszczane są jedynie urządzenia w architekturze nieblokującej pracujące w trybie store-and-forward • Rozmiar tablicy adresów MAC urządzenia min. 32K • Min. przepustowość urządzenia – 320 Gbps • Min. szybkość przekierowań pakietów - 238 Mpps • Pobór mocy urządzenia nie może przekraczać 35W • Przełącznik musi być w formacie 1U umożliwiającym jego montaż w standardowej szafie 19” oraz posiadać w zestawie odpowiednie uchwyty montażowe • Głębokość urządzenia nie może przekraczać 200 mm Standardy: Urządzenie musi spełniać następujące standardy: • 802.3z • 802.3ae • 802.3x • 802.3ad • 802.1ab • 802.1D • 802.1w • 802.1s • 802.1p • 802.1q Funkcjonalność: Wymaga się, aby urządzenie posiadało następujące funkcjonalności: • Zarządzanie za pomocą przeglądarki poprzez interfejs http/https • Z poziomu CLI (Telnet, SSH, port konsoli) musi być możliwa pełna konfiguracja urządzenia • Urządzenie musi mieć obsługiwać możliwość adopcji przez zewnętrzny kontroler w celu scentralizowanego zarządzania • Obsługę stosu IPv4 i IPv6 • Funkcję wykrywania pętli • Funkcję izolacji portów • Funkcję agregacji portów z wykorzystaniem protokołu LACP • Obsługę protokołu LLDP/LLDP-MED • Funkcję DHCP Snooping zarówno dla IPv4 jak i IPv6 • Funkcję umożliwiającą powiązanie adresu IP z adresem MAC (zarówno dla IPv4 jak i IPv6) • Obsługę protokołu drzewa rozpinającego (STP/RSTP/MSTP)

	• Obsługę 4K identyfikatorów VLAN • Funkcję umożliwiającą automatyczne przypisywanie wyznaczonych urządzeń do konkretnej sieci VLAN (MAC VLAN) • IGMP Snooping oraz MLD Snooping • Obsługę min. 900 grup multicastowych jednocześnie • MVR • Obsługę routingu statycznego i/lub dynamicznego • Możliwość konfiguracji co najmniej 16 interfejsów IP • Obsługę min 40 tras statycznych dla funkcji routingu statycznego • Obsługę AAA z wykorzystaniem mechanizmów Radius oraz TACACS+ • Uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia • Obsługę list kontroli dostępu (ACL) • Obsługę SNMP w wersjach v1/v2c/v3 • Obsługę grup RMON 1,2,3,9) Pozostałe wymagania: • Urządzenie musi posiadać certyfikację CE • Gwarancja na urządzenie musi wynosić min. 5 lat • Urządzenie musi pochodzić z polskiego autoryzowanego kanału dystrybucyjnego Ilość: 1 szt. W ofercie proszę podać producenta oraz model.
Przełącznik typ 2	Cechy sprzętowe: • Urządzenie musi być wyposażone w min. 48 gigabitowych portów RJ45 oraz min. cztery porty SFP/SFP+. Nie są dopuszczane porty SFP/SFP+ współdzielone z portami RJ45 (tzw. „combo”) Porty SFP/SFP+ muszą obsługiwać moduły o prędkości transmisji zarówno 1 jak i 10Gbps. • Urządzenie musi posiadać port konsolowy RJ45 lub microUSB • Dopuszczane są jedynie urządzenia w architekturze nieblokującej pracujące w trybie store-and-forward • Rozmiar tablicy adresów MAC urządzenia min. 16K • Przepustowość magistrali dla zadanej minimalnej ilości portów musi wynosić min. 176Gbps • Min. szybkość przekierowań pakietów 130,9 Mpps • Całkowity pobór mocy urządzenia nie może przekraczać 35W • Przełącznik musi być w formacie 1U umożliwiającym jego montaż w standardowej szafie 19” oraz posiadać w zestawie odpowiednie uchwyty montażowe • Głębokość urządzenia nie może przekraczać 230 mm Standardy: Urządzenie musi spełniać następujące standardy: • 802.3i • 802.3u • 802.3z • 802.3ab • 802.3ad • 802.3ae

	• 802.3az • 802.3x • 802.1ab • 802.1D • 802.1w • 802.1s • 802.1p • 802.1q Funkcjonalność: Wymaga się, aby urządzenie posiadało następujące funkcjonalności: • Zarządzanie za pomocą przeglądarki poprzez interfejs http/https • Urządzenie musi mieć obsługiwać możliwość adopcji przez zewnętrzny kontroler w celu scentralizowanego zarządzania • Z poziomu CLI (Telnet, SSH, port konsoli) musi być możliwa konfiguracja wszystkich funkcji urządzenia • Obsługę stosu IPv4 i IPv6 • Funkcję wykrywania pętli • Funkcję izolacji portów • Funkcję agregacji portów z wykorzystaniem protokołu LACP (min. 8 grup, do 8 portów w danej grupie agregacji) • Obsługę protokołu LLDP/LLDP-MED • Funkcję DHCP Snooping zarówno dla IPv4 jak i IPv6 • Funkcję umożliwiającą powiązanie adresu IP z adresem MAC (zarówno dla IPv4 jak i IPv6) • Obsługę protokołu drzewa rozpinającego (STP/RSTP/MSTP) • Obsługę 4K identyfikatorów VLAN • Funkcję umożliwiającą automatyczne przypisywanie wyznaczonych urządzeń do konkretnej sieci VLAN (MAC VLAN) • IGMP Snooping oraz MLD Snooping • Obsługę min. 1000 grup multicastowych jednocześnie • MVR • Obsługę routingu statycznego i/lub dynamicznego • Możliwość konfiguracji co najmniej 16 interfejsów IP • Obsługę min 40 tras statycznych dla funkcji routingu statycznego • Obsługę AAA z wykorzystaniem mechanizmów Radius oraz TACACS+ • Uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia • Obsługę list kontroli dostępu (ACL) • Obsługę SNMP w wersjach v1/v2c/v3 • Obsługę grup RMON 1,2,3,9) Pozostałe wymagania: • Urządzenie musi posiadać certyfikację CE • Gwarancja na urządzenie musi wynosić min. 5 lat • Urządzenie musi pochodzić z polskiego autoryzowanego kanału dystrybucyjnego Ilość: 4 szt. W ofercie proszę podać producenta oraz model.
Przełącznik typ 3	Cechy sprzętowe:

	• Urządzenie musi być wyposażone w min. 48 gigabitowych portów RJ45 oraz min. cztery porty SFP/SFP+. Nie są dopuszczane porty SFP/SFP+ współdzielone z portami RJ45 (tzw. „combo”) Porty SFP/SFP+ muszą obsługiwać moduły o prędkości transmisji zarówno 1 jak i 10Gbps. • Urządzenie musi posiadać port konsolowy RJ45 lub microUSB • Dopuszczane są jedynie urządzenia w architekturze nieblokującej pracujące w trybie store-and-forward • Rozmiar tablicy adresów MAC urządzenia min. 16K • Przepustowość magistrali dla zadanej minimalnej ilości portów musi wynosić min. 176Gbps • Min. szybkość przekierowań pakietów 130,9 Mpps • Porty POE+: Zgodność ze standardami 802.3at/af; • Porty PoE+: min. 48 portów, max. 30 W na każdym porcie • Przełącznik musi być w formacie 1U umożliwiającym jego montaż w standardowej szafie 19” oraz posiadać w zestawie odpowiednie uchwyty montażowe • Głębokość urządzenia nie może przekraczać 230 mm Standardy: Urządzenie musi spełniać następujące standardy: • IEEE 802.1D • IEEE 802.1Q • IEEE 802.1s • IEEE 802.1w • IEEE 802.3ab • IEEE 802.3ae • IEEE 802.3af • IEEE 802.3at • IEEE 802.3i • IEEE 802.3u • IEEE 802.3z Funkcjonalność: Wymaga się, aby urządzenie posiadało następujące funkcjonalności: • Zarządzanie za pomocą przeglądarki poprzez interfejs http/https • Urządzenie musi mieć obsługiwać możliwość adopcji przez zewnętrzny kontroler w celu scentralizowanego zarządzania • Z poziomu CLI (Telnet, SSH, port konsoli) musi być możliwa konfiguracja wszystkich funkcji urządzenia • Obsługę stosu IPv4 i IPv6 • Funkcję wykrywania pętli • Funkcję izolacji portów • Funkcję agregacji portów z wykorzystaniem protokołu LACP (min. 8 grup, do 8 portów w danej grupie agregacji) • Obsługę protokołu LLDP/LLDP-MED • Funkcję DHCP Snooping zarówno dla IPv4 jak i IPv6 • Funkcję umożliwiającą powiązanie adresu IP z adresem MAC (zarówno dla IPv4 jak i IPv6) • Obsługę protokołu drzewa rozpinającego (STP/RSTP/MSTP) • Obsługę 4K identyfikatorów VLAN

	• Funkcję umożliwiającą automatyczne przypisywanie wyznaczonych urządzeń do konkretnej sieci VLAN (MAC VLAN) • IGMP Snooping oraz MLD Snooping • Obsługę min. 1000 grup multicastowych jednocześnie • MVR • Obsługę routingu statycznego i/lub dynamicznego • Możliwość konfiguracji co najmniej 16 interfejsów IP • Obsługę min 40 tras statycznych dla funkcji routingu statycznego • Obsługę AAA z wykorzystaniem mechanizmów Radius oraz TACACS+ • Uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia • Obsługę list kontroli dostępu (ACL) • Obsługę SNMP w wersjach v1/v2c/v3 • Obsługę grup RMON 1,2,3,9) Pozostałe wymagania: • Urządzenie musi posiadać certyfikację CE • Gwarancja na urządzenie musi wynosić min. 5 lat • Urządzenie musi pochodzić z polskiego autoryzowanego kanału dystrybucyjnego Ilość: 1 szt. W ofercie proszę podać producenta oraz model.
Przełącznik typ 4	Cechy sprzętowe: • Urządzenie musi być wyposażone w min. 24 gigabitowych portów RJ45 oraz min. cztery porty SFP. Nie są dopuszczane porty SFP współdzielone z portami RJ45 (tzw. „combo”). • Urządzenie musi posiadać port konsolowy RJ45 lub microUSB • Dopuszczane są jedynie urządzenia w architekturze nieblokującej pracujące w trybie store-and-forward • Rozmiar tablicy adresów MAC urządzenia min. 16K • Przepustowość magistrali dla zadanej minimalnej ilości portów musi wynosić min. 56Gbps • Min. szybkość przekierowań pakietów 41 Mpps • Przełącznik musi być w formacie 1U umożliwiającym jego montaż w standardowej szafie 19” oraz posiadać w zestawie odpowiednie uchwyty montażowe • Głębokość urządzenia nie może przekraczać 330 mm Standardy: Urządzenie musi spełniać następujące standardy: • IEEE 802.3ab • IEEE 802.3i • IEEE 802.3u • IEEE 802.3z Funkcjonalność: Wymaga się, aby urządzenie posiadało następujące funkcjonalności: • Zarządzanie za pomocą przeglądarki poprzez interfejs http/https • Urządzenie musi mieć obsługiwać możliwość adopcji przez zewnętrzny kontroler w celu scentralizowanego zarządzania

	• Z poziomu CLI (Telnet, SSH, port konsoli) musi być możliwa konfiguracja wszystkich funkcji urządzenia • Obsługę stosu IPv4 i IPv6 • Funkcję wykrywania pętli • Funkcję izolacji portów • Funkcję agregacji portów z wykorzystaniem protokołu LACP (min. 8 grup, do 8 portów w danej grupie agregacji) • Obsługę protokołu LLDP/LLDP-MED • Funkcję DHCP Snooping zarówno dla IPv4 jak i IPv6 • Funkcję umożliwiającą powiązanie adresu IP z adresem MAC (zarówno dla IPv4 jak i IPv6) • Obsługę protokołu drzewa rozpinającego (STP/RSTP/MSTP) • Obsługę 4K identyfikatorów VLAN • Funkcję umożliwiającą automatyczne przypisywanie wyznaczonych urządzeń do konkretnej sieci VLAN (MAC VLAN) • IGMP Snooping oraz MLD Snooping • Obsługę min. 256 grup multicastowych jednocześnie • MVR • Obsługę routingu statycznego i/lub dynamicznego • Możliwość konfiguracji co najmniej 16 interfejsów IP • Obsługę min 40 tras statycznych dla funkcji routingu statycznego • Obsługę AAA z wykorzystaniem mechanizmów Radius oraz TACACS+ • Uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia • Obsługę list kontroli dostępu (ACL) • Obsługę SNMP w wersjach v1/v2c/v3 • Obsługę grup RMON 1,2,3,9) Pozostałe wymagania: • Urządzenie musi posiadać certyfikację CE • Gwarancja na urządzenie musi wynosić min. 5 lat • Urządzenie musi pochodzić z polskiego autoryzowanego kanału dystrybucyjnego Ilość: 1 szt. W ofercie proszę podać producenta oraz model.
Przełącznik typ 5	Cechy sprzętowe: • Urządzenie musi być wyposażone w min. 48 gigabitowych portów RJ45 oraz min. cztery porty SFP. Nie są dopuszczane porty SFP współdzielone z portami RJ45 (tzw. „combo”) • Urządzenie musi posiadać port konsolowy RJ45 lub microUSB • Dopuszczane są jedynie urządzenia w architekturze nieblokującej pracujące w trybie store-and-forward • Rozmiar tablicy adresów MAC urządzenia min. 16K • Przepustowość magistrali dla zadanej minimalnej ilości portów musi wynosić min. 104Gbps • Min. szybkość przekierowań pakietów 77 Mpps • Standardy: 802.3af/at • Porty PoE: min. 48 portów, do 30 W na każdym porcie

	• Przełącznik musi być w formacie 1U umożliwiającym jego montaż w standardowej szafie 19” oraz posiadać w zestawie odpowiednie uchwyty montażowe • Głębokość urządzenia nie może przekraczać 330 mm Standardy: Urządzenie musi spełniać następujące standardy: • IEEE 802.1D • IEEE 802.1p • IEEE 802.1s • IEEE 802.1w • IEEE 802.3ad • IEEE 802.3x Funkcjonalność: Wymaga się, aby urządzenie posiadało następujące funkcjonalności: • Zarządzanie za pomocą przeglądarki poprzez interfejs http/https • Urządzenie musi mieć obsługiwać możliwość adopcji przez zewnętrzny kontroler w celu scentralizowanego zarządzania • Z poziomu CLI (Telnet, SSH, port konsoli) musi być możliwa konfiguracja wszystkich funkcji urządzenia • Obsługę stosu IPv4 i IPv6 • Funkcję wykrywania pętli • Funkcję izolacji portów • Funkcję agregacji portów z wykorzystaniem protokołu LACP (min. 8 grup, do 8 portów w danej grupie agregacji) • Obsługę protokołu LLDP/LLDP-MED • Funkcję DHCP Snooping zarówno dla IPv4 jak i IPv6 • Funkcję umożliwiającą powiązanie adresu IP z adresem MAC (zarówno dla IPv4 jak i IPv6) • Obsługę protokołu drzewa rozpinającego (STP/RSTP/MSTP) • Obsługę 4K identyfikatorów VLAN • Funkcję umożliwiającą automatyczne przypisywanie wyznaczonych urządzeń do konkretnej sieci VLAN (MAC VLAN) • IGMP Snooping oraz MLD Snooping • Obsługę min. 256 grup multicastowych jednocześnie • MVR • Obsługę routingu statycznego i/lub dynamicznego • Możliwość konfiguracji co najmniej 16 interfejsów IP • Obsługę min 40 tras statycznych dla funkcji routingu statycznego • Obsługę AAA z wykorzystaniem mechanizmów Radius oraz TACACS+ • Uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia • Obsługę list kontroli dostępu (ACL) • Obsługę SNMP w wersjach v1/v2c/v3 • Obsługę grup RMON 1,2,3,9) Pozostałe wymagania: • Urządzenie musi posiadać certyfikację CE • Gwarancja na urządzenie musi wynosić min. 5 lat • Urządzenie musi pochodzić z polskiego autoryzowanego kanału dystrybucyjnego

	Ilość: 3 szt. W ofercie proszę podać producenta oraz model.
Przełącznik typ 6	Cechy sprzętowe: • Urządzenie musi być wyposażone w min. 24 gigabitowych portów RJ45 oraz min. cztery porty SFP. Nie są dopuszczane porty SFP współdzielone z portami RJ45 (tzw. „combo”). • Urządzenie musi posiadać port konsolowy RJ45 lub microUSB • Dopuszczane są jedynie urządzenia w architekturze nieblokującej pracujące w trybie store-and-forward • Rozmiar tablicy adresów MAC urządzenia min. 16K • Przepustowość magistrali dla zadanej minimalnej ilości portów musi wynosić min. 56Gbps • Min. szybkość przekierowań pakietów 41 Mpps • Standardy: 802.3af/at • Porty PoE+: 24 porty, do 30 W na każdym porcie • Przełącznik musi być w formacie 1U umożliwiającym jego montaż w standardowej szafie 19” oraz posiadać w zestawie odpowiednie uchwyty montażowe • Głębokość urządzenia nie może przekraczać 330 mm Standardy: Urządzenie musi spełniać następujące standardy: • IEEE 802.3ab • IEEE 802.3af • IEEE 802.3at • IEEE 802.3i • IEEE 802.3u • IEEE 802.3z Funkcjonalność: Wymaga się, aby urządzenie posiadało następujące funkcjonalności: • Zarządzanie za pomocą przeglądarki poprzez interfejs http/https • Urządzenie musi mieć obsługiwać możliwość adopcji przez zewnętrzny kontroler w celu scentralizowanego zarządzania • Z poziomu CLI (Telnet, SSH, port konsoli) musi być możliwa konfiguracja wszystkich funkcji urządzenia • Obsługę stosu IPv4 i IPv6 • Funkcję wykrywania pętli • Funkcję izolacji portów • Funkcję agregacji portów z wykorzystaniem protokołu LACP (min. 8 grup, do 8 portów w danej grupie agregacji) • Obsługę protokołu LLDP/LLDP-MED • Funkcję DHCP Snooping zarówno dla IPv4 jak i IPv6 • Funkcję umożliwiającą powiązanie adresu IP z adresem MAC (zarówno dla IPv4 jak i IPv6) • Obsługę protokołu drzewa rozpinającego (STP/RSTP/MSTP) • Obsługę 4K identyfikatorów VLAN

	• Funkcję umożliwiającą automatyczne przypisywanie wyznaczonych urządzeń do konkretnej sieci VLAN (MAC VLAN) • IGMP Snooping oraz MLD Snooping • Obsługę min. 256 grup multicastowych jednocześnie • MVR • Obsługę routingu statycznego i/lub dynamicznego • Możliwość konfiguracji co najmniej 16 interfejsów IP • Obsługę min 40 tras statycznych dla funkcji routingu statycznego • Obsługę AAA z wykorzystaniem mechanizmów Radius oraz TACACS+ • Uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia • Obsługę list kontroli dostępu (ACL) • Obsługę SNMP w wersjach v1/v2c/v3 • Obsługę grup RMON 1,2,3,9) Pozostałe wymagania: • Urządzenie musi posiadać certyfikację CE • Gwarancja na urządzenie musi wynosić min. 5 lat • Urządzenie musi pochodzić z polskiego autoryzowanego kanału dystrybucyjnego Ilość: 2 szt. W ofercie proszę podać producenta oraz model.
Przełącznik typ 7	Cechy sprzętowe: • Urządzenie musi być wyposażone w min. 8 gigabitowych portów RJ45 oraz min. dwa porty SFP (nie dopuszcza się portów SFP współdzielonych z portami RJ45, tzw. portów „combo”) • Co najmniej 8 portów musi dostarczać zasilanie PoE zgodnie ze standardami 802.3af/at z łącznym budżetem PoE min. 140W. • Dopuszczane są jedynie urządzenia w architekturze nieblokującej pracujące w trybie store-and-forward • Rozmiar tablicy adresów MAC urządzenia min. 8K • Min. szybkość przekierowań pakietów 14,88 Mpps • Bufor pakietów min 512KB • Pobór mocy urządzenia nie może przekraczać 180W przy maksymalnym wykorzystaniu budżetu PoE • Przełącznik musi być w formacie 1U umożliwiającym jego montaż w standardowej szafie 19” oraz posiadać w zestawie odpowiednie uchwyty montażowe • Głębokość urządzenia nie może przekraczać 190 mm • Urządzenie musi mieć możliwość pracy w trybie standalone jak również móc być centralnie zarządzanym poprzez kontroler Standardy: Urządzenie musi spełniać następujące standardy: • 802.3i • 802.3u • 802.3ab • 802.3ad • 802.3af

	• 802.3at • 802.3az • 802.3x • 802.1ab • 802.1D • 802.1s • 802.1p • 802.1q • 802.1w Funkcjonalność: Wymaga się, aby urządzenie posiadało następujące funkcjonalności: • Zarządzanie poprzez interfejs graficzny dostępny zarówno poprzez połączenie http jak i https • Urządzenie musi mieć obsługiwać możliwość adopcji przez zewnętrzny kontroler w celu scentralizowanego zarządzania • Zarządzanie poprzez CLI (Telnet, SSH), z poziomu CLI musi być możliwa konfiguracja wszystkich funkcji urządzenia • Obsługę stosu IPv4 i IPv6 • Funkcję wykrywania pętli • Funkcję izolacji portów • Funkcję agregacji portów z wykorzystaniem protokołu LACP • Obsługę protokołu LLDP/LLDP-MED • Funkcję DHCP Snooping zarówno dla IPv4 jak i IPv6 • Funkcję umożliwiającą powiązanie adresu IP z adresem MAC (zarówno dla IPv4 jak i IPv6) • Obsługę protokołu drzewa rozpinającego (STP/RSTP/MSTP) • Obsługę 4K identyfikatorów VLAN • Funkcję umożliwiającą automatyczne przypisywanie wyznaczonych urządzeń do konkretnej sieci VLAN (MAC VLAN) • IGMP Snooping oraz MLD Snooping • MVR • Obsługę routingu statycznego i/lub dynamicznego IPv4 jak i IPv6 • Możliwość konfiguracji co najmniej 16 interfejsów IP • Obsługę min 30 tras statycznych dla funkcji routingu statycznego • Obsługę AAA z wykorzystaniem mechanizmów Radius oraz TACACS+ • Uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia • Obsługę list kontroli dostępu (ACL) • Obsługę SNMP w wersjach v1/v2c/v3 Obsługę grup RMON 1,2,3,9 Pozostałe wymagania: • Urządzenie musi posiadać certyfikację CE • Gwarancja na urządzenie musi wynosić min. 5 lat • Urządzenie musi pochodzić z polskiego autoryzowanego kanału dystrybucyjnego Ilość: 6 szt. W ofercie proszę podać producenta oraz model.

Kontroler sprzętowy	Cechy fizyczne: • Kontroler musi umożliwiać zarządzanie punktami dostępowymi w liczbie min 450. • Kontroler musi mieć możliwość zarządzania zarówno urządzeniami odpowiadającymi za segment bezprzewodowy sieci (punkty dostępowe) jak i urządzeniami tworzącymi warstwę dostępową i szkielet sieci (przełączniki) • Urządzenie musi być wyposażone w min. 2 porty RJ45 o prędkości 10/100/1000Mb/s • Urządzenie musi być wyposażone w port USB umożliwiający podłączenie zewnętrznego nośnika danych • Urządzenie musi mieć możliwość montażu w szafie rack 19”, elementy montażowe muszą być zawarte w zestawie. • Urządzenie musi posiadać następujące certyfikaty: CE, RoHS • Dopuszczana temperatura pracy urządzenia musi zawierać się w przedziale od 0 do 40 stopni Celsjusza Cechy funkcjonalne: • Urządzenie musi umożliwiać automatyczne wykrywanie wszystkich urządzeń w sieci lokalnej kompatybilnych z Kontrolerem • Urządzenie musi zapewniać możliwość zdalnego zarządzania siecią w danej lokalizacji wykorzystując chmurę lub inny mechanizm pozwalający na dostęp do kontrolera z dowolnego miejsca • W zakresie ogólnej funkcjonalności urządzenie musi wspierać funkcje: o Wyświetlania topologii sieci (wykorzystując urządzenia zarządzane przez kontroler) o Zarządzania wieloma lokalizacjami z poziomu pojedynczego kontrolera o ACL (listy kontroli dostępu) zarówno dla użytkowników łączących się do sieci przewodowo jak i bezprzewodowo o Uwierzytelniania użytkowników zarówno przewodowych jak i bezprzewodowych z wykorzystaniem strony powitalnej • W zakresie konfiguracji sieci WiFi urządzenie musi umożliwiać konfigurację następujących funkcji: o Multi SSID o Sieć dla Gości (odizolowanie klientów w tej sieci od innych klientów lokalnych bez wykorzystania VLAN) o Powiązanie SSID do VLAN o Filtrowanie adresów MAC (tryby blacklist/whitelist) o Kanał transmisji/moc nadawania konkretnych AP o Równoważenie obciążenia punktów dostępowych o Sterowanie pasmem o Ograniczenie prędkości transmisji o Tworzenie harmonogramu sieci WiFi oraz resetu urządzeń o QoS o Harmonogramowanie sieci bezprzewodowej oraz restartu urządzenia Pozostałe wymagania: • Urządzenie musi posiadać certyfikację CE • Gwarancja na urządzenie musi wynosić min. 5 lat • Urządzenie musi pochodzić z polskiego autoryzowanego kanału dystrybucyjnego Ilość: 1 szt. W ofercie proszę podać producenta oraz model.

Wdrożenie i konfiguracja	1. Zamawiający wymaga aby Wykonawca wykonał w sieci Zamawiającego pełne mapowanie połączeń między poszczególnymi urządzeniami jego sieci. W ramach prac przewidzianych na tym etapie realizacji usługi wymaga się aby inwentaryzacja objęła: a. Inwentaryzację szaf telekomunikacyjnych. b. Inwentaryzację paneli krosowniczych (Patchpaneli). c. Inwentaryzację przełączników zarządzalnych oraz niezarządzalnych w szkielecie sieci LAN. d. Inwentaryzację urządzań kluczowych w sieci Zamawiającego. e. Inwentaryzację połączeń między gniazdami dostępowymi w pomieszczeniach Zamawiającego oraz poszczególnymi paneli krosowniczych oraz przełącznikami w szkielecie sieci LAN. f. Opracowanie dokumentu opisującego wykaz połączeń w sieci Zamawiającego. g. Opracowanie koncepcji podziału sieci na podsieci, z uwzględnieniem ograniczeń wynikających z powstałej mapy połączeń. 2. Zamawiający wymaga aby Wykonawca wykonał w sieci Zamawiającego rekonfigurację połączeń sieciowych, tak aby jej finalny podział pozwalał na segmentację sieci na poszczególne segmenty. W ramach prac przewidzianych na tym etapie realizacji usługi wymaga się aby Wykonawca: a. Wykonał niezbędne kopie zapasowe dla urządzeń w szkielecie sieci LAN (UTM/przełączniki). b. Dokonał rekonfiguracji urządzenia klasy UTM pod kątem wykreowania podsieci sieci LAN zgodnie z wykazem i zaakceptowaną koncepcją segmentacji. c. Przeprowadził rekonfigurację urządzenia klasy UTM pod kątem obsługi usług DHCP oraz DNS dla poszczególnych podsieci. d. Stworzył na urządzeniu klasy UTM reguły ruchu sieciowego pozwalającego na niezbędną komunikację sieciową. e. Dokonał rekonfiguracji przełączników zarządzalnych pod kątem wykreowania podsieci sieci LAN zgodnie z wykazem i zaakceptowaną koncepcją segmentacji. f. Przypisze odpowiednie podsieci do poszczególnych portów przełączników zarządzalnych. g. Wykona weryfikację poprawności komunikacji dla poszczególnych portów przełączników zarządzalnych. h. Opracuje finalną dokumentację opisującej segmentację sieci LAN
wyposażenie umożliwiające zmianę sposobu fizycznej realizacji układu połączeń sieci typ 1	Typ Interfejsu SFP+ Przepływność min. 10G Długość kabla min. 2 m Typ modułu Duplex Gwarancja min .24 miesiące Ilość: 12 szt.
wyposażenie umożliwiające zmianę sposobu fizycznej realizacji układu połączeń sieci typ 2	Typ Interfejsu SFP+ Przepływność min. 10G Długość kabla min. 3 m Typ modułu Duplex Gwarancja min .24 miesiące Ilość: 4 szt.
Termin realizacji	Dostawa do 90 dni od dnia podpisania umowy Wdrożenie i konfiguracja: do 30 września 2025 r.

3. Serwer

Producent: ……

Model: ……..

Ilość: 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków 3.5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. • Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 56 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. • Płyta główna powinna obsługiwać do 8TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane dwa procesory min. 8-rdzeniowe klasy x86, min. 2.6GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 170 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	Minimum 128GB
Funkcjonalność pamięci RAM	• Demand Scrubbing, • Patrol Scrubbing, • Permanent Fault Detection (PFD)
Gniazda PCI	Min. 8 slotów PCIe w tym minimum 6 slotów FH
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)

Dyski twarde	• Zainstalowane:
	  ○ 4x dysk NLSAS o pojemności min. 4TB, 12Gb, Hot-Plug
	  ○ 2x dysk SSD SATA o pojemności min. 960GB, 6Gb, Hot-Plug

Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający
	  ○ Min. 8GB nieulotnej pamięci cache,
	  ○ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
	  ○ Wsparcie dla dysków samoszyfrujących

Wbudowane porty	• 4x USB, w tym min. 1 porty USB 3.0 • 2x port VGA (jeden na panelu przednim) • Możliwość rozbudowy o Serial Port
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne, Hot-Plug
Zasilacze	Redundantne, Hot-Plug min. 1100W klasy Titanium
System operacyjny/dodatkowe oprogramowanie	Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na zaoferowanym serwerze. Wymaga się aby oferowane licencje umożliwiały korzystanie 50 użytkownikom. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9) 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).

	10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15) Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18) Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty z certyfikatami (smartcard), c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25) 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: I. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, II. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, III. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. IV. 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 e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: I. Dystrybucję certyfikatów poprzez http II. Konsolidację CA dla wielu lasów domeny, III. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, IV. 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) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wsparcie dla algorytmów Suite B (RFC 4869), 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 do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: I. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

	II. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. III. Obsługi 4-KB sektorów dysków IV. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra V. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. VI. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 26) 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. 27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ○ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; ○ możliwość podmontowania zdalnych wirtualnych napędów; ○ wirtualną konsolę z dostępem do myszy, klawiatury; ○ wsparcie dla IPv6; ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;

	○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie; ○ wsparcie dla dynamic DNS; ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)

	○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami – załączyć do ofert dokumentację techniczną potwierdzającą spełnienie normy lub oświadczenie producenta serwera o spełnieniu normy. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. • Wszystkie certyfikaty należy dołączyć do oferty
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Min 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta • Możliwość rozszerzenia gwarancji przez producenta do 7 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych) • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.

	• Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
Termin realizacji	Dostawa do 90 dni od dnia podpisania umowy

4. Rekonfiguracja usługi domenowej Active Directory

Ilość: 1 szt.

Nazwa	Wymagane parametry techniczne
Opis	W ramach postępowania Wykonawca zoptymalizuje, zabezpieczy i dostosuje strukturę AD do aktualnych i przyszłych potrzeb organizacyjnych. Zakres prac: 1. Audyt Obecnej Infrastruktury AD • Przeprowadzenie szczegółowego audytu obecnej infrastruktury Active Directory. • Identyfikacja obecnych problemów, nieprawidłowości oraz obszarów wymagających optymalizacji. 2. Projekt Nowej Struktury AD • Opracowanie nowej struktury AD, uwzględniającej najlepsze praktyki w zakresie bezpieczeństwa, wydajności i skalowalności. • Przygotowanie planu migracji i rekonfiguracji z minimalnym wpływem na bieżące funkcjonowanie organizacji. 3. Rekonfiguracja i Optymalizacja • Rekonfiguracja struktury AD zgodnie z zaakceptowanym założeniami. • Optymalizacja konfiguracji serwerów domenowych, ról, replikacji i polityk grupowych. • Przeprowadzenie migracji obiektów (użytkowników, grup, jednostek organizacyjnych) do nowej struktury. 4. Zabezpieczenie Infrastruktury AD • Wdrożenie zaawansowanych polityk bezpieczeństwa AD. • Konfiguracja logowania i monitorowania działań w AD. • Wdrożenie mechanizmów zabezpieczających przed nieautoryzowanym dostępem i atakami. Termin wykonania prac do 30 września 2025.

5. UTM - Licencja

Producent: ……..

Model: ……..

Ilość: 1 szt.

Nazwa	Wymagane parametry techniczne
Opis	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres realizacji projektu tj. do dnia 07.04.2026r. Do posiadanego przez Zamawiającego urządzenia Fortinet Fortigate 200F. System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden z inżynierów musi posiadać najwyższy stopień certyfikacji) oraz ISO 9001 w zakresie serwisowania urządzeń informatycznych. Wszystkie certyfikaty należy dołączyć do oferty. Termin dostarczenia licencji do 30 dni od dnia podpisania umowy. Licencje ważne od dnia 22.08.2024r.

6. Oprogramowanie do wykonywania kopii bezpieczeństwa

Producent: ……..

Model: ……..

Ilość: 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. Licencja wieczysta dla 5 serwerów (fizyczne i VM) z dwuletnim gwarancją producenta oprogramowania szt. 3.
Wymagania szczegółowe	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time) Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji

	Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
Wymagania RPO	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
Wymagania RTO	Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.

	Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle

	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Wymagania ograniczenia ryzyka	Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
Wymagania dla Agenta	Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE Rozwiązanie musi wspierać system operacyjny macOS Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów Rozwiązanie musi wspierać backup podłączonych dysków USB Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone Rozwiązanie musi wspierać kontrolę pasma sieciowego Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN

	Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft Rozwiązanie musi wspierać technologię BitLocker Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform Rozwiązanie musi wspierać szyfrowanie Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
Termin realizacji	Dostawa do 90 dni od dnia podpisania umowy

7. Oprogramowanie do zbierania i analizy logów

1. Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń:
   a. System operacyjny powinien być na licencji Open Source.
   b. Platformą sprzętowa dla rozwiązania centralnego składowania dzienników jest w sieci Zamawiającego wirtualna maszyna w środowisku Vmware.
   c. Architektura systemu powinna bazować na komponentach o licencjonowaniu Open Source
   d. Zamawiający na wyżej wymieniony cel planuje przeznaczyć maszynę wirtualną o parametrach procesor (CPU) 8 rdzeni, pamięć RAM 16 GB oraz dysk twardy (HDD) min. 2TB.
   e. Tworzenie użytkowników w systemie centralnego składowania logów może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.
   f. System centralnego składowania dzienników zdarzeń powinien mieć możliwość zdefiniowania dowolnie wielu i dowolnie skonfigurowanych źródeł danych, wśród których znajdują się m.in.: Sysloga UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Konfiguracja źródeł danych powinna pozwalać na zdefiniowanie dowolnego portu komunikacji, np. Syslog UDP 514 lub/i Syslog UDP 10514.
   g. System centralnego składowania dzienników zdarzeń powinien mieć możliwość ekstrakcji fragmentów wpisów logów z możliwością wykorzystania ich do filtrowania danych, budowania zapytań dla powiadomień i alarmów czy widoków w ramach dashboardów oraz ich import jak i eksport.

h. System centralnego składowania dzienników zdarzeń powinien udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trypie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV czy urządzeniach z dowolną przeglądarką WWW.
i. System centralnego składowania dzienników zdarzeń powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego.
j. System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów).

2. W zakresie wdrożenie proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego zbierania i analizy logów:
   a. Instalacja systemu operacyjnego na wybranej przez Zamawiającego maszynie wirtualnej.
   b. Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do Centralnego systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca zaproponuje rozwiązanie pozwalające na uspójnienie zegarów czasów sieci Zamawiającego.
   c. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracja parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.
   d. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów obowiązujących aktów prawnych i dobrych praktyk występujących w środowisku Zamawiającego.
   e. Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły:
      i. (5x) Urządzenie klasy UTM firmy Stormshield
      ii. (1x) Urządzenie klasy UTM firmy Fortigate
      iii. (6x) Kontroler Ubiquiti UCK wraz z podłączonymi do nich punktami AP
      iv. Przełączniki zarządzalne zgodnie z pkt 2 OPZ
      v. (15x) Serwery Windows
      vi. (1x) Serwery Linux
      vii. (420x) stacji roboczych Windows7, 10 i 11
      viii. (1x) Konsolę centralnego zarządzania Bitdefender Cloud Zone
      ix. (4x) Serwer wirtualizacji VMware ESXI
      x. (1x) Serwer zarządzania wirtualizacją VMware vCenter
      xi. (1x) Aplikację Axence nVision
      xii. (2x) Macierze dyskowe
      xiii. (3x) Urządzenia NAS
      xiv. (6x) UPS
      xv. (2x) Centrala alarmowa
      xvi. Kontrolery zdalnego dostępu do serwerów (iDRAC, iMana)
   f. Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.
   g. Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.

h. Rekonfiguracja posiadanego rozwiązania Axence nVision poprzez modyfikacje monitorowanych zasobów i usług oraz sposobów powiadamiania o istotnych zdarzeniach w tych zasobach.
i. Wykonanie całkowitej rekonfiguracji rozwiązania Axence nVision w celu umożliwienia interakcji między rozwiązaniami, która umożliwi przesyłanie i analizę logów z wyżej wymienionego rozwiązania. Rekonfiguracja ma umożliwić pobieranie logów takich jak:
    i. Aktywność Administratorów w konsoli centralnego zarządzania, z klasyfikacją wykonanych czynności;
    ii. Listę zdarzeń co do których nVision ogłasza alarm, z klasyfikacją na typ zdarzenia, istotność oraz źródło problemu;
j. Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.
k. Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.
l. Konfiguracja wysyłania powiadomień poprzez maila lub Microsoft Teams w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.
m. Wprowadzenie pracowników działu IT do obsługi wdrożonego systemu.

3. Wykonawca zrealizuje prace do dnia 30 września 2025 r.
4. Gwarancja i asysta techniczne:
    a. Zamawiający wymaga aby Wykonawca w czasie od wdrożenia do okresu realizacji projektu tj. 07.04.2026 r. zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.
    b. Zamawiający wymaga aby Wykonawca w czasie od wdrożenia do okresu realizacji projektu tj. 07.04.2026 r. świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów.
    c. Zamawiający wymaga aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 16.00.
    d. Zamawiający akceptuje fakt, ze każda interwencja wymagać będzie od niego zgłoszenia potrzeby pomocy drogą elektroniczną, a wskazany kanał komunikacji będzie wyznaczony przez Wykonawcę, i może to być system zgłoszeń elektronicznych lub komunikacja mailowa.
5. Zamawiający wymaga aby Wykonawca zorganizował i przeprowadził w swojej siedzibie lub innym miejscu nie zależnym od Zmawiającego konsultacje z zarządzenia i administracji wdrożonego systemu.
6. Zamawiający wymaga aby usługa konsultacji została zrealizowana w terminie do 3 miesięcy od wdrożenia usługi.
7. Konsultacje udzielone zostaną dwóm pracownikom Zamawiającego.
8. Zamawiający wymaga aby w trakcie konsultacji realizowane były ćwiczenia opisujące codzienną pracę administracyjną z wdrożonym systemem, rozwiązywaniem problemów, procedurę aktualizacji rozwiązania oraz rozbudowy o dodatkowe widoki i kanały napływu danych.
9. Wymagana zagadnienia konsultacyjne:
    a. Wstęp do zarządzania logami
    b. System centralnego składowania logów – wymagania, architektura oraz różnice w wersjach
    c. Instalacja i konfiguracja ogólnych ustawień systemu centralnego składowania logów
    d. Zbieranie logów, czyli konfiguracja metod pozyskiwania dzienników zdarzeń.
    e. Przetwarzanie dzienników zdarzeń, czyli tworzenie strumieni logów, ich parsowanie oraz filtrowanie

f. Wizualizacja logów czyli tworzenie czytelnych zestawień tabelarycznych i graficznych
g. Konfiguracja alertów i powiadomień.
h. Administracja i utrzymanie systemu centralnego składowania logów
i. Case Study czyli praktyczne przykłady użycia systemu centralnego składowania logów

10. Zamawiający wymaga aby konsultacje zamykały się w ramach czasowych 2 dni roboczych (2x 7 godz.)

Adam Dariusz Rachuba

Elektronicznie podpisany przez Adam Dariusz Rachuba
Data: 2024.08.05 12:08:47 +02'00'