Opis przedmiotu zamówienia

Spis treści

Wstęp

Wymagania ogólne dla dostarczanego sprzętu i oprogramowania (dotyczy wszystkich systemów opisanych w tym dokumencie):

a) Opisane parametry techniczne są wymaganiami minimalnymi i wykonawca może zaoferować urządzenia o parametrach lepszych niż wymagane,
b) Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów z obszaru Unii Europejskiej,
c) Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by nie były używane
d) Sprzęt musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis) kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej;
e) Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa);
f) Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich;
g) Zamawiający dopuszcza realizację poszczególnych grup funkcjonalnych przez zespoły urządzeń pod następującymi warunkami:
   i. połączenie urządzeń będzie zrealizowane w sposób nie ograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu, jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność urządzenia),
   ii. łączna wielkość zestawu nie będzie przekraczać wymaganej wielkości urządzenia,
   iii. zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zespołu urządzeń,
   iv. wszystkie elementy zestawu będą spełniały wymagania związane z zarządzaniem,
   v. Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ±10%, 50Hz;

Storage (1 szt.)

Macierz dyskowa

Lp.	Nazwa elementu	Minimalne wymagane parametry
1.	Obudowa	1) Przez macierz dyskową Zamawiający rozumie zestaw dysków twardych HDD i/lub dysków SSD kontrolowanych przez minimum pojedynczą parę kontrolerów macierzowych, które kontrolują wszystkie zasoby dyskowe macierzy z poziomu pojedynczej konsoli WebGUI/CLI administratora; 2) Macierz musi posiadać architekturę modułową w zakresie obudowy dla instalacji kontrolerów oraz obsługiwanych dysków, z dopuszczeniem współdzielenia jednego z modułów przez kontrolery i dyski dla zapisów danych Użytkownika; 3) System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie; 4) Kontrolery w głównym module macierzy muszą być ze sobą połączone bez konieczności korzystania z okablowania zewnętrznego,

Lp.	Nazwa elementu	Minimalne wymagane parametry
		5) Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia); 6) Każdy moduł/obudowa macierzy powinna posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii; 7) Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy; 8) Moduły dla dalszej rozbudowy o dodatkowe dyski i przestrzeń dyskową muszą zapewniać gęstości upakowania co najmniej 24 dysków 2,5" lub co najmniej 12 dysków 3,5" na każde 2U przestrzeni instalacyjnej w szafie przemysłowej rack standardu 19"; 9) Dostarczona konfiguracja macierzy musi pozwalać na połączenie kaskadowe lub w układzie pętli pomiędzy modułem bazowym a dodatkowymi półkami dyskowymi, z wykorzystaniem minimum 2-torów kablowych w tych połączeniach – okablowanie to musi być zgodne ze standardem SAS 12Gb/s. 10) W przypadku braku obsługi połączeń w układzie pętli dopuszcza się jako alternatywne rozwiązanie macierz z zainstalowanymi 4 kontrolerami RAID;
2.	Pojemność	1) Oferowana macierz musi obsługiwać min. 220 dysków wykonanych w technologii hot-plug – jeżeli dla obsługi tej funkcjonalności konieczny jest zakup dodatkowych licencji to należy ją dostarczyć wraz z macierzą; 2) Obsługa liczby dysków jak powyżej musi być zapewniona zarówno w zakresie dysków HDD jak i SSD 3) Wszystkie zainstalowane dyski hot-plug, muszą być dostępne dla zapisu danych Użytkownika; 4) Jeżeli pojemność któregoś z dysków jest wykorzystywana na tzw. potrzeby własne macierzy (zapis zawartości pamięci podręcznej Cache, oprogramowanie wewnętrzne, firmware macierzy, itp.) to nie można go wliczać do wymaganej pojemności macierzy oraz wymaganej liczby dysków, ani jako dysk zapasowy hot-spare
3.	Kontrolery	1) Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami; 2) Każdy z kontrolerów macierzy musi posiadać po minimum 32 GB pamięci podręcznej Cache 3) Kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (Cache Mirror) przeznaczonych do zapisu; 3) Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 1,2TB poprzez instalację dodatkowych modułów pamięci Flash w kontrolerach lub wykorzystanie pojemności zainstalowanych w macierzy dysków SSD dedykowanych do tego celu, 4) W przypadku awarii zasilania dane przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik; 5) Kontrolery muszą posiadać możliwość ich wymiany w przypadku awarii lub planowych zadań utrzymaniowych bez konieczności wyłączania zasilania całego urządzenia – w przypadku konfiguracji z min. 2 kontrolerami; 6) Każdy z kontrolerów RAID powinien posiadać dedykowane minimum 1 interfejs RJ-45 Ethernet 1Gbps i 1 port USB 2.0 lub minimum 2 porty RJ-45

Lp.	Nazwa elementu	Minimalne wymagane parametry
		Ethernet 1Gbps - dla zdalnej komunikacji z oprogramowaniem zarządzającym macierzą; 7) Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej; 8) Każdy kontroler macierzy musi pozwalać na konfigurację interfejsów niezbędnych dla współpracy w sieci IP/FC/SAS SAN oraz NAS; 9) Dla obsługi operacji blokowych I/O w sieci IP/FC/SAS SAN kontrolery macierzy muszą wspierać protokoły transmisji: FC 32/16Gb/s , iSCSI 10/1Gb/s, SAS 12Gb/s; 10) Dla obsługi operacji plikowych I/O w sieci NAS kontrolery macierzy muszą wspierać minimum protokoły dostępu: CIFS, NFS - - licencja na wymienioną funkcjonalność NIE JEST przedmiotem niniejszego postępowania 11) Kontrolery macierzy muszą obsługiwać do 128 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów;
4.	Interfejsy	1) Oferowana macierz musi mieć minimum 4 porty FC16Gbps wyposażonych we wkładki światłowodowe multi-mode przeznaczone do dołączenia serwerów, wyprowadzone po 2 porty na każdy kontroler macierzy 2) Macierz musi mieć możliwość rozbudowy do minimum 16 portów FC16Gbps SFP+ – jeżeli dla spełnienia wymagania konieczne jest dostarczenie dodatkowych licencji to należy je zaoferować wraz z macierzą. 3) Macierz musi umożliwiać wymianę zaoferowanych portów dla hostów na porty obsługujące następujące protokoły: FC 32Gbps, iSCSI 10Gbps, SAS12Gbps; 4) Wymiana portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu - macierz ma być dostarczona z aktywną licencją na instalację i obsługę każdego z wymienionych protokołów transmisji danych;
5.	Poziomy RAID	1) Macierz musi zapewniać poziom zabezpieczenia danych na dyskach, definiowany poziomami RAID: 0, 1, 10, 5, 50, 6; 2) Macierz musi pozwalać na jednoczesną obsługę wspieranych poziomów RAID 3) Macierz musi wspierać mechanizm przyspieszonej odbudowy danych konfigurowanych w grupę RAID zapewniającą dostęp do danych w przypadku jednoczesnej awarią minimum 2 fizycznych dysków w takiej grupie.
6.	Wspierane dyski	1) Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex; 2) Oferowana macierz musi wspierać dyski hot-plug: - dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS12Gb/s i SAS6Gb/s - dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm i 10 krpm, 3) Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD 4) Model macierzy musi pozwalać na instalację dysków hot-plug w formacie 2,5” i 3,5”; 5) Wymagane jest dostarczenie macierzy zawierającej min. 8 dysków SAS SSD pojemności minimum 3,84TB każdy 6) Zaoferowane dyski SAS SSD musza być dedykowane do zastosowań enterprise i posiadać parametr DWPD1 lub wyższy 6) Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug w trybach: globalny dysk zapasowy, dedykowany dysk zapasowy

Lp.	Nazwa elementu	Minimalne wymagane parametry
		7) W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować konieczności powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk 8) Dostarczona macierz w oferowanej konfiguracji umożliwia szyfrowanie danych kluczem minimum 256bit na zainstalowanych dysków - jeżeli funkcjonalność ta wymaga dodatkowych elementów sprzętowych bądź aktywacji dodatkowej licencji to należy dostarczyć je wraz z rozwiązaniem dla maksymalnej pojemności macierzy.
7.	Opcje software'owe	1) Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 8 kopii migawkowych, z możliwością późniejszej rozbudowy do obsługi min 4000 migawek; 2) Macierz musi umożliwiać zdefiniowanie min. 8000 woluminów (LUN); 3) Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy; 4) Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową; 5) Macierz musi posiadać wsparcie dla systemów operacyjnych : MS Windows Server 2019/2022, SuSE Linux, Oracle Linux, Oracle VM, RedHat Linux, Vmware. 6) Macierz musi obsługiwać natywne mechanizmy multipath systemów Windows Server i Linux SuSE/RedHat – jeżeli dedykowane oprogramowanie multipath jest oferowane bezpłatnie musi być możliwość jego pobrania ze strony internetowej producenta macierzy; 7) Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC oraz iSCSI z posiadanymi przez Zamawiającego macierzami **Fujitsu DX200S5**, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji – licencja na wymienioną funkcjonalność NIE JEST przedmiotem niniejszego postępowania; 8) Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – licencja na wymienioną funkcjonalność NIE JEST przedmiotem niniejszego postępowania; 9) Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy; 10) Model oferowanej macierzy musi wspierać rozwiązania klasy 'klastra macierzowego' tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software'owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2

Lp.	Nazwa elementu	Minimalne wymagane parametry
		macierzami – licencja na wymienioną funkcjonalność NIE JEST przedmiotem niniejszego postępowania; 11) Macierz musi obsługiwać mechanizmy automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi (tzw. automated storage tiering) na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych podłączonych serwerów, środowisk i aplikacji – licencja na wymienioną funkcjonalność NIE JEST przedmiotem niniejszego postępowania 12) Mechanizm jw. musi być obsługiwany przy korzystaniu zarówno z trzech jak i z dwóch dostarczonych technologii dyskowych: SSD, SAS, NLSAS; 13) Mechanizm automatycznej migracji danych musi pozwalać na wykluczanie definiowanych okien czasowych (np. weekend, dni świąteczne, dowolny dzień) z analizy wydajności jak w pkt.11. 14) Macierz musi posiadać możliwość zastosowania mechanizmów redukcji zajętości danych typu deduplikacja/kompresja dla danych zapisywanych na każdym typie wspieranej technologii dyskowej 15) Mechanizmy redukcji zajętości danych jw. muszą obsługiwane co najmniej w trybie online (tj. przed pierwszym zapisem danych na dyskach macierzy) w sposób selektywny per LUN i z dowolną kombinacją każdego z typów redukcji.
8.	Konfiguracja, zarządzanie	1) Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej zarówno przy obsłudze transmisji danych protokołami blokowymi (FC, iSCSI, SAS) jak i do obsługi transmisji protokołami CIFS/NFS; 2) Oprogramowanie zarządzające musi być dostarczone w wariancie dla maksymalnej obsługiwanej pojemności dyskowej macierzy oraz dla maksymalnej liczby dysków wspieranej przez oferowaną macierz; 3) Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. 4) Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora; 5) Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI ;
9.	Gwarancja i serwis	1) 3 lata gwarancji producenta macierzy w trybie onsite z gwarantowanym czasem reakcji rozumianej jako przybycie serwisu do miejsca instalacji macierzy najpóźniej w następnym dniu roboczym od zgłoszenia usterki. Wymagane jest pisemne poświadczenia gotowości realizacji wymaganego poziomu serwisowego przez polskie przedstawicielstwo producenta macierzy. W okresie objętym gwarancją producenta uszkodzone dyski pozostają własnością Zamawiającego i nie są przekazywane do organizacji serwisowej producenta

Lp.	Nazwa elementu	Minimalne wymagane parametry
		2) Elementy, z których zbudowana jest macierz muszą być produktami producenta tej macierzy lub być przez niego certyfikowane dla oferowanego modelu macierzy 3) Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania dostarczonego, które są elementem zamówienia, w ciągu 36 miesięcy od daty zakupu; 4) Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązania bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy przez okres min. 24 kolejnych miesięcy; 5) Macierz musi pochodzić z legalnego kanału sprzedaży producenta w Polsce nie dopuszcza się użycia macierzy re-fabrykowanych, po-demonstracyjnych lub powystawowych; 6) Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia; 7) Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać pełen adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje;

Przełącznik FC (2szt.)

1. Przełącznik FC musi być wykonany w technologii FC minimum 32 Gbs i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, 4 Gbs w zależności od rodzaju zastosowanych wkładek SFP.
2. Dostarczony przełącznik FC musi być wyposażony w 24 porty FC. Aktywnych portów FC 16szt., wszystkie aktywne porty obsadzone wkładkami SFP+ 16Gbs SWL.
3. Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika wyposażonej we wkładki 32Gbs mogą pracować równocześnie z pełną prędkością 32Gb/s.
4. Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji wyposażonej we wkładki 32Gbs musi wynosić minimum 760Gb/s end-to-end.
5. Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 785ns.
6. Rodzaj obsługiwanych portów, co najmniej: E, D oraz F.
7. Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) I szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. Wraz z przełącznikiem należy dostarczyć odpowiedni zestaw montażowy do szafy 19”.
8. Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 24 aktywne porty 32Gbps to 80W.
9. Maksymalna ilość ciepła wydzielanego przez przełącznik FC wyposażony w 24 aktywne porty 32Gbps to 215 BTU na godzinę.
10. Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.
11. Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą).
12. Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa:
    - uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP I FCAP

- uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP
- szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2.
- definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control)
- definiowane kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+
- szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS
- obsługa SNMP v1 oraz v3
- IP Filter dla portu administracyjnego przełącznika
- wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP
- wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP

13. Przełącznik FC musi mieć możliwość konfiguracji przez:
    - polecenia tekstowe w interfejsie znakowym konsoli terminala
    - przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie.
14. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, Serial oraz inband IP-over-FC.
15. Przełącznik FC musi zapewniać obsługę protokołu NVMe over FC.
16. Przełącznik FC musi zapewniać obsługę interfejsu zarządzającego REST API.
17. Wsparcie dla N_Port ID Virtualization (NPIV).
18. Urządzenie musi być dostosowane do pracy w środowisku o wilgotności zawierającej się między 10% a 90% oraz temperaturze otoczenia między 2 stopnie Celsiusa a 40 stopni Celsiusa.
19. Aktywne funkcje: Active Gateway, Webtools, Advanced Zoning, FullFabric (z obsługą do min. 128 przełączników FC). Możliwość obsługi dodatkowych funkcjonalności (przez zakupienie odpowiednich licencji): Trunking, Extended Fabric, Fabric Vision
20. Gwarancja:
    - 3 lat gwarancji producenta
    - Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w dni robocze w godzinach 9:00 – 16:00 następującymi kanałami: telefonicznie oraz przez Internet

Elementy dodatkowe

Zamawiający wymaga dostarczenia i instalacji dodatkowych komponentów:

1. 3 sztuki kontrolerów LAN 2x10GB SFP+ do serwerów Dell R540, porty obsadzone modułami 10GbE SR
2. 2 sztuki kontrolerów LAN 2x10GB SFP+ do serwerów Dell R740, porty obsadzone modułami 10GbE SR
3. Wznowienie gwarancji producenta do 2 posiadanych serwerów Dell R540 do 06/11/2026
4. Wznowienie gwarancji producenta do 3 posiadanych serwerów Dell R740 do 13/05/2026

Serwer backup (1szt.)

Obudowa

- Typu RACK, wysokość 2U;
- Szyny umożliwiające wysunięcie serwera z szafy stelażowej
- Możliwość zainstalowania 10 dysków twardych hot plug 3,5”;
- Możliwość rozbudowy o fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
- Zainstalowane 2 szt. dysków SSD SATA 480GB Hot-Plug oraz 6 szt. 12TB SATA Hot Plug;
- Możliwość zainstalowania dysku M.2 NVMe PCIe4.0 x4;
- Zainstalowany wewnętrzny napęd optyczny umożliwiający zapisanie 25GB danych na jednym nośniku.

Płyta główna

- Dwuprocesorowa;
- Wyprodukowana i zaprojektowana przez producenta serwera;
- Możliwość instalacji procesorów 60-rdzeniowych;
- Zainstalowany moduł TPM 2.0;
- 6 złącz PCI Express generacji 5 w tym:
  - 4 fizyczne złącza o prędkości x16;
  - 2 fizyczne złącza o prędkości x8;
  - Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
  - Opcjonalnie możliwość uzyskania 9 aktywnych interfejsów PCI-e;
- 32 gniazda pamięci RAM;
- Obsługa minimum 8 TB pamięci RAM DDR5;
- Wsparcie dla technologii:
  - Memory Scrubbing;
  - SDDC;
  - ECC;
  - Memory Mirroring;
  - ADDDC;
- Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.

Procesory

- Dwa procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86_64;
- Osiągające w teście SPEC CPU2017 Integer Rate wynik SPECrate2017_int_base 172 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla dowolnego serwera z oferty producenta.

Pamięć RAM

- 128 GB pamięci RAM;
- DDR5 Registered 4800MT/s;

Kontrolery LAN

Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:

- 5x 1Gbit Base-T;
- Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;

Interfejsy LAN zainstalowany w slotach PCI Express:

- 4x 10Gbit SFP+ obsadzone modułami 10Gbit SR.

Kontrolery I/O

- Kontroler SAS RAID dla dysków wewnętrznych posiadający 4GB pamięci cache zabezpieczonej przed utratą danych w przypadku zaniku zasilania, obsługujący poziomy RAID: 0,1,10,5,50,6,60
- Karta 1x 16Gb FC

Porty

- Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
- 2 porty USB 3.0 dostępne z tyłu serwera;
- 2 porty USB 3.0 na panelu przednim;
- Możliwość rozbudowy o 1 port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
- Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

Zasilanie, chłodzenie

- Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W;
- Redundantne wentylatory hotplug.

Zarządzanie

- Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;
    - informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
        - karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;
        - procesory CPU;
        - pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
        - nośnik pamięci M.2 SSD;
        - status karty zarządzającej serwera;
        - wentylatory;
        - bateria podtrzymująca ustawienia BIOS płyty głównej;
        - zasilacze;
        - system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);
- Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
    - Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
    - Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
    - Dostęp poprzez przeglądarkę Web, SSH;
    - Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
    - Zarządzanie alarmami (zdarzenia poprzez SNMP);
    - Możliwość przejęcia konsoli tekstowej;
    - Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
    - Obsługa serwerów proxy (autentykacja);
    - Obsługa VLAN;
    - Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
    - Wsparcie dla protokołu SSDP;
    - Obsługa protokołów TLS 1.2, SSL v3;
    - Obsługa protokołu LDAP;
    - Integracja z HP SIM;
    - Synchronizacja czasu poprzez protokół NTP;
    - Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;
- Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
- Wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
- Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

Wspierane OS

- Microsoft Windows Server 2022, 2019;

- VMWare vSphere 8.0;
- Suse Linux Enterprise Server 15;
- Red Hat Enterprise Linux 9, 8;
- Microsoft Hyper-V Server 2019.

Gwarancja

- 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia z opcją pozostawienia zepsutych dysków u klienta. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.
- Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w systemie helpdesk/servicedesk producenta sprzętu;
- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
- Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
- Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).

Dokumentacja, inne

- 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 – wymagane oświadczenie wykonawcy lub producenta;
- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;
- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;
- W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
- Zgodność z normami: CB, RoHS, WEEE oraz CE.

Biblioteka taśmowa LTO

1.1. Urządzenie musi posiadać konstrukcję modułową o zajętości maksymalnie 3U w przestrzeni instalacyjnej szafy przemysłowej standardu 19” dla każdego modułu. Moduły muszą posiadać kompletny zestaw akcesoriów (szyny montażowe, mocowania szyn montażowych) pozwalających na ich instalację w standardowej szafie przemysłowej RACK.

1.2. Każdy moduł biblioteki musi posiadać redundancje układów zasilania.

1.3. Moduł biblioteki musi pozwalać na instalację minimum 3 napędów taśmowych standardu LTO oraz 40 nośników taśmowych LTO – oferowany moduł musi posiadać zainstalowany magazynek lub magazynki dla wszystkich obsługiwanych nośników (tj. dla 40 sztuk).

1.4. Jeżeli sloty na nośniki taśmowe wymagają aktywacji to wszystkie dostarczone sloty muszą być aktywowane dla minimum 20 szt.

1.5. Biblioteka musi pozwalać na rozbudowę o kolejne moduły dla obsługi łącznie min. 280 zainstalowanych nośników LTO oraz do minimum 21 napędów taśmowych typu LTO.

1.6. Moduł główny biblioteki musi posiadać panel operatora wyposażony w wyświetlacz LCD pozwalający na wykonanie podstawowych operacji konfiguracji ustawień biblioteki, inwentaryzacji taśm, testowanie biblioteki, robotyki i napędów, relokacji nośników taśmowych w ramach partycji, czyszczenie napędów z użyciem nośników czyszczących, sprawdzanie zawartości logów zbierających informacje o awariach sprzętowych i błędów w obsłudze napędów i nośników, konfiguracji parametrów koniecznych dla ustawienia

zdalnego zarządzania biblioteką poprzez sieć LAN.

1.7. Panel operatora musi posiadać możliwość blokady operacji konfiguracyjnych poprzez zabezpieczenie hasłem lub kodem PIN.

1.8. Każdy moduł biblioteki musi posiadać możliwość wymiany lub uzupełniania nośników taśmowych bez przerywania pracy napędów taśmowych tzw. Mailslot – wymagana jest możliwość jednoczesnej operacji wymiany/uzupełnienia dla minimum 5 nośników taśmowych LTO.

1.9. Biblioteka musi być wyposażona w minimum jeden interfejs Ethernet RJ-45 obsługujący prędkości transmisji 10/100/1000Mb/s dla zdalnego zarządzania biblioteką oraz w interfejsy USB wyprowadzone na front i tył obudowy głównego modułu biblioteki dla zapisu i wgrywania parametrów konfiguracyjnych oraz wgrywania nowego oprogramowania wewnętrznego elementów biblioteki.

1.10. Biblioteka musi być wyposażona w czytnik kodów kreskowych pozwalający na automatyczną inwentaryzację zainstalowanych nośników taśmowych LTO posiadających etykiety z takim kodem.

1.11. Każdy moduł biblioteki musi pozwalać na mieszaną konfigurację obsługiwanych napędów LTO.

1.12. Biblioteka musi jednocześnie obsługiwać napędy taśmowe LTO-7 i LTO-8.

1.13. Biblioteka musi jednocześnie obsługiwać napędy LTO j.w. wyposażone w interfejsy FC 8Gb/s i SAS 6Gb/s.

1.14. Każdy zainstalowany napęd taśmowy LTO musi obsługiwać minimum dwie generacje nośników LTO w zakresie operacji odczytu i zapisu danych.

1.15. Wymagane jest dostarczenie min. 1 napędu LTO8 FC.

1.16. Wymagane jest dostarczenie min. 1 nośnika czyszczącego.

1.17. Wraz z urządzeniem wymagane jest dostarczenie min. 10 nośników danych LTO8 wraz z dedykowanymi kodami kreskowymi.

1.18. Biblioteka taśmowa musi obsługiwać mechanizmy partycjonowania logicznego swoich zasobów z możliwością zdefiniowania do minimum 21 partycji –licencji dla aktywowania tej funkcjonalności nie jest wymagana.

1.19. Licencja dla partycjonowania logicznego oferowanej biblioteki musi bazować na programowym aktywowaniu tej funkcjonalności tj. bez konieczności zakupu dodatkowych elementów sprzętowych – w innym przypadku należy dostarczyć wraz z biblioteką wszystkie elementy sprzętowe niezbędne dla późniejszego aktywowania mechanizmów partycjonowania logicznego.

1.20. Biblioteka musi wspierać mechanizmy szyfrowania danych na nośnikach taśmowych LTO-6 i LTO-7 i LTO-8 z poziomu aplikacji do wykonywania kopii zapasowych.

1.21. Biblioteka musi wspierać protokół KMIP (Key Management Interoperability Protocol) dla bezpiecznego przesyłania kluczy szyfrujących poprzez sieć LAN, nie wymagane jest dostarczenie licencji dla aktywowania tej funkcjonalności.

1.22. Biblioteka musi pozwalać na wykonywanie operacji administratorskich zdalnie poprzez sieć LAN w trybie Web-GUI z poziomu standardowej przeglądarki WWW.

1.23. Biblioteka musi obsługiwać komunikacje z szyfrowaniem transmisji protokołem SSL.

1.24. Biblioteka musi obsługiwać protokół SNMP v.1/2/3 oraz adresację zgodną ze standardem IPv.4 i IPv.6 dla modułu zdalnego zarządzania.

1.25. Biblioteka musi obsługiwać tryb automatycznego powiadamiania o błędach i zdarzeniach krytycznych poprzez wysyłanie wiadomości e-mail oraz poprzez wysyłanie komunikatów SNMP do uprawnionej stacji administratora obsługującej zarządzanie na platformie SNMP.

1.26. Gwarancja:

1.26.1. Biblioteka musi być objęta minimum 36 miesięcznym okresem gwarancji producenta urządzenia.

1.26.2. Naprawy będą realizowane w trybie NBD 9x5 w miejscu instalacji urządzenia.

1.26.3. Przyjmowanie zgłoszeń serwisowych musi odbywać się w trybie 24/7 – w ciągu 24 godzin przez 7 dni w tygodniu.

1.26.4. Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji

oprogramowania wbudowanego, które są elementem zamówienia, w ciągu okresu gwarancji od daty zakupu.

1.26.5. Bezpłatna, gwarantowana skuteczna naprawa w miejscu instalacji urządzenia będzie realizowana najpóźniej w następnym dniu roboczym od zgłoszenia usterki.

1.26.6. Wraz z biblioteką należy zapewnić subskrypcję na bezpłatną aktualizację (możliwość bezpłatnego pobrania ze stron internetowych producenta) oprogramowania wewnętrznego biblioteki (tzw. firmware) w całym okresie obowiązywania gwarancji.

1.27. Urządzenie musi pochodzić z legalnego kanału sprzedaży producenta w Polsce. Nie dopuszcza się użycia elementów i podzespołów biblioteki oferowanych jako refabrykowane, podemonstracyjne lub powystawowe.

System operacyjny

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz 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 oferowanym serwerze, licencja dożywotnia nie może być ograniczona czasowo.

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
    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.
31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Oprogramowanie backup

1) Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji
    a) Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012
    b) Vmware vSphere min. w wersjach v5.5-7.0.3
    c) Nutanix AHV 5.15, 5.20 (LTS)
    d) Maszyny fizyczne: Windows Server 2022, 2019, 2016, 2012R2, 2012
    e) Microsoft 365 (Exchange online, One Drive for Business, Sharepoint, Teams)
2) Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V
3) Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:
    a) na serwerze Windows lub Linux
    b) jako maszyna wirtualna Vmware
    c) jako maszyna wirtualna Amazon
    d) na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital
4) Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS
5) Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania

6) Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
7) Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności
8) W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie **12 miesięcy** wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania
9) W ramach dostawy wymagane jest dostarczenie licencji na ochronę **10 gniazd** procesorów w hostach Vmware lub Hyper-V
10) Oprogramowanie musi posiadać funkcje backupu i replikacji:
    a) Backup maszyn wirtualnych Vmware
    b) Replikacja maszyn wirtualnych Vmware (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
    c) Backup maszyn wirtualnych Hyper-V
    d) Replikacja maszyn wirtualnych Hyper-V (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
    e) Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
    f) Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
    g) Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
    h) Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
    i) "Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych
    j) Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem"
    k) Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
    l) Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
    m) Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach
11) Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
    a) Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
    b) Kompresja backupu, w tym konfigurowalny stopień kompresji
    c) Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne
12) Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
    a) Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
    b) Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
    c) Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji:
    d) Microsoft Exchange 2013, 2016, 2019

e) Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022
f) Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
g) Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
h) Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
i) Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji

13) Oprogramowanie musi posiadać poniższe funkcje:
a) Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
b) Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)
c) Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
d) Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
e) Microsoft Exchange
f) MS Active Directory
g) MS SQL
h) Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.

14) Oprogramowanie do backupu musi pozwalać na:
a) Tworzenie backupu I replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
b) Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
c) Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN
d) Akceleracje sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
e) Wsparcie dla urządzeń oferujących dodatkową deduplikację danych

15) Oprogramowanie musi pozwalać na następujące formy zarządzania:
a) Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
b) Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
c) Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania
d) Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.
e) Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
f) Oprogramowanie musi umożliwiać integrację z Active Directory
g) Oprogramowanie musi wspierać tzw. tryb multi tenant, umożliwiający podzielenie oprogramowania do backupu na kilka podinstancji zarządzanych z odrębnych interfejsów w celu rozłożenia zarządzania w złożonych środowiskach

System EDR (1 kpl.)

Zamawiający posiada system antywirusowy ESET PROTECT Essential liczba stanowisk: 130**.** W ramach zadania należy zwiększyć funkcjonalność systemu antywirusowego do wersji ESET PROTECT Enterprise zawierającej moduł EDR oraz zwiększyć do **140 stanowisk** i przedłużyć licencję do **2026-06-30.** Wykonawca może zaoferować nowy system EDR który będzie spełniał poniższe funkcjonalności:

Administracja zdalna w chmurze

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych

oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
• tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
• tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
• tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika

poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
• tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
• tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
• tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
• tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących

się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
Dodatkowe wymagania dla ochrony serwerów Linux:
18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

a. usunięcie zawartości urządzenia,
b. przywrócenie urządzenie do ustawień fabrycznych,
c. zablokowania urządzenia,
d. uruchomienie sygnału dźwiękowego,
e. lokalizację GPS.
6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
a. nazwę aplikacji,
b. nazwę pakietu,
c. kategorię sklepu Google Play,
d. uprawnienia aplikacji,
e. pochodzenie aplikacji z nieznanego źródła.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
a) Czysty,
b) Podejrzany,
c) Bardzo podejrzany,
d) Szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

Moduł XDR

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica".
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
16. Konsola administracyjna musi mieć możliwość tagowania obiektów.
17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

Przełącznik iSCSI (1szt.)

1. Wysokość urządzenia 1U
2. Przełącznik posiadający minimum 24 porty 10GBase-X (SFP+)
3. Przełącznik posiadający minimum 2 porty QSFP28
4. Przełącznik posiadający miejsce na dodatkowy moduł mogący, w zależności od potrzeb, być obsadzonym:
   - 4 portami 1/10GBase-X (SFP+)
   - 4 portami 10/25GBase-X (SFP28)
5. Nieblokującą architekturę o wydajności przełączania min. 1080 Gb/s
6. Szybkość przełączania min. 800 Milionów pakietów na sekundę
7. Wielkość tablicy MAC minimum 40k wpisów
8. Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management
9. Wbudowany port USB oraz port konsoli
10. Przełącznik musi posiadać wbudowane, redundantne zasilacze 230V AC
11. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
12. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
13. Obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym)
14. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora. System musi mieć możliwość dodania nowego modułu lub aktualizacji już zaimplementowanych bez konieczności restartu całego urządzenia
15. Możliwość monitorowania zajętości CPU
16. Routing statyczny
17. Obsługa routingu dynamicznego IPv4
    a. RIPv1/v2
    b. OSPFv2, BGP, IS-IS– jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania
18. Policy Based Routing dla IPv4
19. Tablica routing IPv4 minimum 15k wpisów
20. Obsługa routingu dynamicznego dla IPv6
    a. RIPng,
    b. OSPFv3, BGP, IS-IS– jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania
21. Policy Based Routing dla IPv6
22. Tablica routing IPv6 minimum 7k wpisów
23. Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)
24. Obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping
25. Obsługa protokołu PIM-SM
26. Obsługa Network Login
    a. IEEE 802.1x
    b. Web-based Network Login
    c. MAC based Network Login
27. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www)
28. Obsługa wielu klientów (min. 12) Network Login na jednym porcie (Multiple supplicants)
29. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reauthentykacji dołączonego klienta z systemu NAC
30. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
31. Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu

pasma

32. Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie:
    a. definicji sieci VLAN,
    b. reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,
    c. realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,
    d. realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
33. Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) – również per-command Authentication
34. Bezpieczeństwo MAC adresów:
    a. ograniczenie liczby MAC adresów na porcie
    b. zatrzaśnięcie MAC adresu na porcie
    c. możliwość wpisania statycznych MAC adresów na port/vlan
    d. możliwość wyłączenia MAC learning
35. Zabezpieczenie przełącznika przed atakami DoS
    a. Networks Ingress Filtering RFC 2267
    b. SYN Attack Protection
    c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
36. Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika – wire-speed)
37. Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation
38. Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard
39. Obsługa redundancji routingu VRRP (RFC 2338) i VRRPv2 (RFC 3768)
40. Obsługa STP, RSTP, MSTP, PVST+
41. Obsługa protokołu MVRP
42. Obsługa EAPS (RFC 3619)
43. Obsługa protokołu ERPS lub równoważnego oraz ITU G.8032
44. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP
45. Obsługa IEEE 802.3ah Ethernet OAM
46. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników
47. Musi mieć możliwość zarządzania za pomocą SSH/Telnet, SNMP, oraz systemu zarządzania dostarczonego przez producenta
48. Zarządzanie przez SNMP v1/v2/v3
49. Obsługa SYSLOG z możliwością definiowania wielu serwerów
50. Sprzętowa obsługa sFlow lub protokołu równoważnego
51. Obsługa RMON (RFC 1757) i RMON2 (RFC 2021)
52. Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)
53. Możliwość uruchamiania skryptów:
    a. Ręcznie
    b. O określonym czasie lub co wskazany okres czasu
    c. Na podstawie wpisów w logu systemowym
54. Obsługa XML API poprzez Telnet/SSH i HTTP/HTTPS
55. Obsługa Data Center Bridging
    a. Data Center Bridging Exchange Protocol (DCBx)
    b. Priority Flow Control (PFC)
56. Obsługa protokołu MACSEC (IEEE 802.1AE) – jeżeli funkcjonalność ta wymaga dodatkowych modułów lub licencji Zamawiający nie wymaga ich dostarczenia w ramach tego postępowania
57. Usługi wirtualizacji warstwy L2 i L3
    a. Przełącznik musi udostępniać możliwość wirtualizacji usług sieciowych w warstwie L2 i L3 modelu OSI.
    b. Przełącznik musi zapewniać „multi-tennancy" dla usług sieciowych zarówno w L2 jak i L3. Rozumiemy przez to przypadek, w którym do przełącznika doprowadzone są nakładające się

numery VLAN (vlan overlap) lub podsieci IP (subnet overlap). W takim przypadku przełącznik musi zapewniać izolację tego ruchu od siebie.

c. Przełącznik musi zapewniać usługi zwirtualizowane L2 i L3 w oparciu o standardowe protokoły sieciowe (SPB 802.1aq lub EVPN)
d. Przełącznik musi umożliwiać skonfigurowanie usług wirtualizacji w L2
e. Przełącznik musi umożliwiać obsługę usług multicast dla L2 jak i L3 bez konieczności używania protokołu PIM.
f. Przełącznik musi zapewniać możliwość zastosowania dowolnej topologii połączeń przy współpracy z innymi urządzeniami tworzącymi węzły sieci szkieletowej.
g. Przełącznik musi zapewniać możliwość dokładania nowych węzłów w sieci bez wpływu na już działające usługi sieciowe.

58. Dożywotnia gwarancja producenta uwzględniająca:
    a. wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego,
    b. aktualizacje oprogramowania układowego (firmware),
    c. dostęp do bazy wiedzy oraz dokumentacji technicznej producenta.
59. Wraz z przełącznikiem należy dostarczyć 24 sztuki kompatybilnych modułów SFP+ SR 10Gbs 850nm LC DDM

Wdrożenie

Storage

a) Instalacja urządzeń w szafie rack
b) Aktualizacja oprogramowania układowego do najnowszej wersji
c) Podłączenie do sieci SAN za pomocą interfejsów SFP+
d) Konfiguracja podłączenia do sieci zarządzania w nowo zamontowanych urządzeniach
e) Instalacja dodatkowych kart LAN w posiadanych serwerach
f) Instalacja i konfiguracja przełączników FC, podłączenie do infrastruktury serwerowej z zachowaniem redundancji połączeń
g) Utworzenie ZONE i aliasów i konfiguracji produkcyjnej
h) Rekonfiguracja serwerów oraz posiadanych macierzy dyskowych w celu komunikacji protokołem FC
i) Relokacja i konfiguracja przełączników dla obsługi sieci storage oraz lan za pomocą interfejsów SFP+ posiadanych przez Zamawiającego
j) Przegląd i rekonfiguracja posiadanych serwerów wirtualnych w celu usprawnienia pracy poszczególnych serwisów serwowanych przez Zamawiającego.
k) Migracja serwerów w celu uzyskania najlepszej wydajności dla obsługi poszczególnych usług realizowanych przez Zamawiającego.

Serwer backup

a) Instalacja serwera i biblioteki taśmowej w szafie rack
b) Instalacja i konfiguracja dostarczonego systemu backup
c) Podłączenie serwera do sieci LAN z wykorzystaniem interfejsów 10GB SFP+
d) Konfiguracja podłączenia do sieci zarządzania w nowo zamontowanych urządzeniach
e) Połączenie serwera do przełączników LAN
f) Podłączenie biblioteki i serwera z wykorzystaniem interfejsu FC
g) Instalacja systemu na dostarczonym środowisku
h) Instalacja komponentów na potrzeby pracy z oprogramowaniem kopii zapasowych
i) Konfiguracja połączeń z hypervisorami maszyn wirtualnych, magazynów danych, transporterów
j) Konfiguracja zadań kopii bezpieczeństwa
k) Konfiguracja systemu zgodnie z najlepszymi praktykami producenta

l) Kopie zapasowe maszyn wirtualnych muszą być wykonywane bezagentowo
m) Jako repozytorium dla systemu kopii zapasowych, należy wykorzystać macierz typu NAS i wewnętrzne dyski serwera
n) Konfiguracja replikacji wybranych serwerów i usług na posiadaną infrastrukturę Zamawiającego.

System EDR

a) Inicjalizacja konsoli zarządzania
b) Instalacja na przykładowym komputerze klienta EDR
c) Dystrybucja klienta z wykorzystaniem GPO
d) Konfiguracja VSS
e) Konfiguracja polityki bezpieczeństwa

Przełącznik iSCSI

a) Instalacja urządzenia w szafie rack
b) Aktualizacja oprogramowania układowego do najnowszej wersji
c) Podłączenie do sieci SAN za pomocą interfejsów 10GB SFP+

Signature Not Verified
Dokument podpisany przez Marek Chojnowski
Data: 2024.10.02 13:27:23 CEST