Załącznik nr 1 do umowy

(3.1) OPROGRAMOWANIE DO CENTRALNEGO SKŁADOWANIA I ANALIZOWANIA LOGÓW SYSTEMOWYCH WRAZ Z WDROŻENIEM, WSPARCIEM I SZKOLENIEM Z ZAKRESU SKŁADOWANIA I ANALIZOWANIA LOGÓW SYSTEMOWYCH DLA INFORMATYKÓW

Opis przedmiotu zamówienia (OPZ)

1. **Wymagania związane z rozwiązaniem centralnego składowania logów systemowych (dziennika zdarzeń):**
   1) System operacyjny powinien być na licencji Open Source.
   2) Platformą sprzętowa dla rozwiązania centralnego składowania logów jest w sieci Zamawiającego fizyczny serwer będący na wyposażeniu Zamawiającego |wirtualna maszyna w środowisku Vmware | wirtualna maszyna w środowisku Hyper-V.
   3) Architektura systemu powinna bazować na komponentach **o licencjonowaniu Open Source.**
   4) Zamawiający na wyżej wymieniony cel planuje przeznaczyć rozwiązanie sprzętowe | maszynę wirtualną o parametrach procesor (CPU) 8 rdzeni, pamięć RAM 16 GB oraz dysk twardy (HDD) 2TB.
   5) 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.
   6) System centralnego składowania logów systemowych 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.
   7) System centralnego składowania logów systemowych 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.
   8) System centralnego składowania logów systemowych 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.
   9) System centralnego składowania logów systemowych powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego.
   10) System centralnego składowania logów systemowych powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów).
2. **W zakresie wdrożenia proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania logów systemowych:**

1) Instalacja systemu operacyjnego na wybranych przez Zamawiającego serwerze fizycznym | maszynie wirtualnej.

2) Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do Centralnego systemu składowania logów systemowych. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca zaproponuje rozwiązanie pozwalające na uspójnienie zegarów czasów sieci Zamawiającego.

3) Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracją parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.

4) Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktów prawnych i dobrych praktyk występujących w środowisku Zamawiającego.

5) Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania logów systemowych (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły:

   a) (2x) Urządzenie klasy UTM firmy watchguard.
   b) (20X) Przełączniki zarządzalne firmy MiKroTik, Dell, HP.
   c) (12x) Serwery Windows.
   d) (10x) Serwery Linux.
   e) (250) stacji roboczych Windows 10 i 11 - z możliwością zmiany ilości o +/- 10% stacji.
   f) (3x) Serwer wirtualizacji VMware ESX.
   g) (1x (Serwer zarządzania wirtualizacją VMware vCenter.
   h) (1x) Aplikację Axence nVision.

6) Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.

7) Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.

8) Automatyzacja analizy napływających logów poprzez zbudowanie dashboardów generujących i prezentujących dane w postaci tabelarycznej i/lub graficznej.

9) Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.

10) Konfiguracja wysyłania powiadomień poprzez maila lub Microsoft Teams w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.

11) Wprowadzenie pracowników działu IT do obsługi wdrożonego systemu.

3. Szkolenie w formie warsztatu:

1) Zamawiający wymaga, aby Wykonawca przeprowadził w siedzibie Zamawiającego warsztaty techniczne z zarządzania i administracji wdrożonego systemu.

2) **Zamawiający wymaga przeszkolenia w formie warsztatów dla 3 uczestników.**

3) Zamawiający wymaga, aby w trakcie warsztatów realizowane były ćwiczenia opisujące codzienną pracę administracyjną z wdrożonym systemem, rozwiązywaniem problemów, procedurę aktualizacji rozwiązania oraz rozbudowy o dodatkowe widoki i kanały napływu danych.

4) Wymagana agenda warsztatów:

   a) Wstęp do zarządzania logami.

b) Wymagania oraz architektura wdrożonego rozwiązania.

c) Instalacja i konfiguracja ogólnych ustawień.

d) Zbieranie logów, czyli konfiguracja metod pozyskiwania dzienników zdarzeń.

e) Przetwarzanie logów systemowych, 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 wdrożonego rozwiązania.

i) Case Study czyli praktyczne przykłady użycia.

5) Zamawiający wymaga, aby warsztaty (szkolenie) zamykały się w ramach czasowych **2 dni roboczych (2x 7 godzin zegarowych) z trzema przerwami po 15 minut.**

6) Zamawiający wymaga, aby warsztaty (szkolenie) kończyły się potwierdzeniem uczestnictwa **w formie certyfikatu**.

4. Gwarancja i wsparcie techniczne:

1) Zamawiający wymaga, aby Wykonawca w **czasie do 30.04.2026 r. zapewnił wsparcie techniczne** polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.

2) Zamawiający wymaga, aby Wykonawca **w czasie do 30.04.2026 r. świadczył wsparcie techniczne w zakresie aktualizacji zarówno systemu, jak i jego komponentów.**

3) Zamawiający wymaga, aby w/w usługi były świadczone **od poniedziałku do piątku** między godzinami **8:00 a 16:00.**

4) Zamawiający akceptuje fakt, że 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.

(3.2) PRZEPROWADZENIE SEGMENTACJI SIECI

Opis przedmiotu zamówienia (OPZ)

1. Zamawiający wymaga, aby Wykonawca wykonał w sieci Zamawiającego pełne mapowanie połączeń między poszczególnymi urządzeniami jego sieci **w 3 lokalizacjach Urzędu na terenie miasta Bełchatowa.** W ramach prac przewidzianych na tym etapie realizacji usługi wymaga się, aby inwentaryzacja objęła:
   1) Inwentaryzację szaf telekomunikacyjnych.
   2) Inwentaryzację paneli krosowniczych (Patchpaneli).
   3) Inwentaryzację przełączników zarządzalnych oraz niezarządzalnych w szkielecie sieci LAN.
   4) Inwentaryzację urządzań kluczowych w sieci Zamawiającego.
   5) Inwentaryzację połączeń między gniazdami dostępowymi w pomieszczeniach Zamawiającego oraz poszczególnymi panelami krosowniczymi oraz przełącznikami w szkielecie sieci LAN.
   6) Opracowanie dokumentu opisującego wykaz połączeń w sieci Zamawiającego.
   7) 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:
   1) Wykonał niezbędne kopie zapasowe dla urządzeń w szkielecie sieci LAN (UTM/przełączniki).
   2) Dokonał rekonfiguracji urządzeń klasy UTM pod kątem wykreowania podsieci sieci LAN zgodnie z wykazem i zaakceptowaną koncepcją segmentacji.
   3) Przeprowadził rekonfigurację urządzenia klasy UTM pod kątem obsługi usług DHCP oraz DNS dla poszczególnych podsieci.
   4) Stworzył na urządzeniu klasy UTM reguły ruchu sieciowego pozwalającego na niezbędną komunikację sieciową.
   5) Dokonał rekonfiguracji przełączników zarządzalnych pod kątem wykreowania podsieci sieci LAN zgodnie z wykazem i zaakceptowaną koncepcją segmentacji.
   6) Przypisał odpowiednie podsieci do poszczególnych portów przełączników zarządzalnych.
   7) Wykonał weryfikację poprawności komunikacji dla poszczególnych portów przełączników zarządzalnych.
   8) Opracował finalną dokumentację opisującą segmentację sieci LAN.
3. Zamawiający wymaga, aby Wykonawca skonfigurował w ramach usługi segmentacji sieci alarmy i powiadomienia umożliwiające obserwacje ruchu sieciowego wraz z wykrywaniem podejrzanych zachowań.
4. Zamawiający wymaga, żeby Wykonawca udzielił **6 miesięcznej gwarancji na usługę w zakresie realizacji zgłoszeń z nieprawidłowościami w działaniu i konfiguracji sieci LAN.**
5. Zamawiający wymaga, aby prace wykonywane były poza godzinami pracy Urzędu, zaczynały się w **piątek po godzinie 15:00 i kończyły się w niedzielę - nie później niż godzina 18:00.**

Dodatkowo Zamawiający wymaga, aby Wykonawca pozostał stacjonarnie do dyspozycji Zamawiającego przez kolejne **2 dni w godzinach pracy Urzędu (7:00 - 18:00),** w celu natychmiastowej reakcji na ewentualne problemy techniczne zgłaszane przez pracowników Urzędu.

(3.3) OPROGRAMOWANIE DO SKANOWANIA PODATNOŚCI WRAZ ZE WSPARCIEM TECHNICZNYM I SZKOLENIEM DLA INFORMATYKÓW W ZAKRESIE SYSTEMU ZARZĄDZANIA PODATNOŚCIAMI (3 OSOBY)

Opis przedmiotu zamówienia (OPZ)

Licencja:

1. **Licencja musi być dostarczona w formie usługi rozliczanej jednorazowo.**
2. Licencja musi umożliwiać sposób rozliczenia w oparciu o chronione stacje robocze, serwery fizyczne, maszyny wirtualne, aplikacje chmurowe lub w przeliczeniu na GB chronionych danych.
3. Licencja musi gwarantować obsługę minimum 25 maszyn wirtualnych w obszarze ochrony Backup & Recovery oraz **230 licencji dla skanowania podatności** i zarządzania aktualizacjami.
4. **Licencja musi być ważna do 30.04.2026 r.**
   1) Zamawiający wymaga, aby Wykonawca w **czasie do 30.04.2026 r. zapewnił wsparcie techniczne** polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.
   2) Zamawiający wymaga, aby Wykonawca **w czasie do 30.04.2026 r. świadczył wsparcie techniczne w zakresie aktualizacji zarówno systemu, jak i jego komponentów.**

Konsola centralnego zarządzania:

1. Konsola zarządzania ulokowana w chmurze Producenta dostarczonego rozwiązania.
2. Konsola zarządzania i dokumentacja do niej dostępna w polskiej wersji językowej, z możliwością płynnej zmiany na minimum język angielski.
3. Konsola zarządzania ulokowana w polskim Data Center Producenta.
4. Dostęp do konsoli zarządzania możliwy ze wsparciem dla wieloskładnikowego uwierzytelniania (MFA)
5. Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek WWW.
6. Zarządzanie procesem ochrony dla wielu różnych podsieci, również w przypadku stosowania NAT.
7. Zdalna instalacja agentów na maszynach z systemem operacyjnym Windows.
8. Zdalne uaktualniania agentów dla środowisk Windows, Linux oraz hostów wirtualizacji Hyper-V i VMware.
9. Możliwość automatycznej aktualizacji agentów, bez potrzeby tworzenia i konfiguracji zadań aktualizacji.
10. Automatyczna aktualizacja ma pozwalać na określenie okna serwisowego, w którym może być wykonywana.
11. Konsola musi umożliwiać grupowania chronionych urządzeń w celu precyzyjnego adresowania polityk pracy dla agenta.
12. Konsola powinna pozwalać definiować powiadomienia mailowe oraz w interfejsie konsoli zarządzania informować o odstępstwach od właściwej pracy systemu.

Funkcje podstawowe platformy cyberbezpieczeństwa:

1. Wykrywanie konfiguracji sprzętowej chronionego urządzenia dla minimum urządzeń z systemem operacyjnym Windows 7 SP1 i nowsze edycje oraz Windows Server 2012R2 i nowsze.

2. Wykrywanie luk w oparciu o metodykę CVE Mitre (Common Vulnerabilities and Exposures) dla systemów operacyjnych urządzeń z klientem platformy działających pod kontrolą minimum Windows 7 SP1 i nowsze edycje oraz Windows Server 2012R2 i nowsze.
3. Wykrywanie luk w oparciu o metodykę CVE Mitre (Common Vulnerabilities and Exposures) dla aplikacji zainstalowanych na urządzeniach z klientem platformy działających pod kontrolą minimum Windows 7 SP1 i nowsze edycje oraz Windows Server 2012R2 i nowsze.
4. Połączenie zdalne do chronionego urządzenia z użyciem protokołu RDP dla urządzeń Windows 7 SP1 i nowsze edycje oraz Windows Server 2012R2 i nowsze.
5. Podstawowa ochrona przed szkodliwym szyfrowaniem plików na chronionym urządzeniu dla minimum urządzeń z systemem operacyjnym Windows 7 SP1 i nowsze edycje oraz Windows Server 2012R2 i nowsze.
6. Zarządzanie nośnikami zewnętrznymi podłączanymi do chronionych urządzeń dla minimum urządzeń z systemem operacyjnym Windows 7 SP1 i nowsze edycje oraz Windows Server 2012R2 i nowsze. Przez zarządzanie Zamawiający rozumie nadawanie uprawnień odczyt lub odczyt-zapis dla wybranych i autoryzowanych nośników oraz blokowania pozostałych.

Funkcje modułu „Backup & Recovery”

1. W skład modułu zarządzania wykonywania kopii zapasowych Zamawiający wymaga, aby wchodziły następujące funkcjonalności:
   1) Tworzenie kopii zapasowych w oparciu o kopie pełne, różnicowe oraz przyrostowe.
   2) Tworzenie kopii zapasowych w oparciu o harmonogram bazujący na minimum miesiącach, tygodniach, dniach i godzinach.
   3) Tworzenie kopii zapasowych całego chronionego urządzenia (tzw. Bear Metal), wybranych dysków, folderów i plików.
   4) Szyfrowanie kopii zapasowych w oparciu o algorytm AES-256.
   5) Możliwość zapisu kopii zapasowych w zasobach sieciowych Zamawiającego ze wsparciem protokołów SMB, NFS.
   6) Możliwość weryfikacji użyteczności kopii zapasowych w automatycznych testach bazujących na odzyskaniu kopii urządzenia jako maszyny wirtualnej wraz z pobraniem zrzutu ekranu logowania maszyny lub pulsu życia urządzenia odzyskanego.
   7) Odtworzenie całej chronionej maszyny uwzględnionej w kopii zapasowej na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową.
   8) Tworzenie kopii zapasowej stacji roboczych pod kontrolą systemów operacyjnych Windows (XP SP1 i nowsze) oraz MacOS (10.13 i nowsze).
   9) Tworzenie kopii zapasowej fizycznych serwerów pod kontrolą systemów operacyjnych Windows (2003 i nowsze) oraz Linux (Red Hat 4.x i nowsze, Ubuntu 9.10 i nowsze, Debian 4.x i nowsze).
   10) Tworzenie kopii zapasowych maszyn niezależnie od środowiska wirtualizującego.
   11) Bezagentowe tworzenie kopii zapasowych maszyn wirtualnych pod kontrolą środowisk wirtualizujących VMware (pod kontrolą vCenter) oraz Hyper-V.
   12) Przestrzeń chmurowa możliwa do wyboru jako jedna z lokalizacji docelowych powinna spełniać poniższe wymagania:

a) Kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich repliki muszą być przechowywane na terenie Polski.
b) Producent przechowuje dane osobowe klienta (dane osobowe oraz kopie zapasowe) przy użyciu technik szyfrowania, minimum AES-256.
c) Infrastruktura (chmurowy magazyn kopii zapasowych) jest zaprojektowana zgodnie z podejściem N+1 (to, co niezbędne +1).
d) Producent oprogramowania jest zgodny z standardem bezpieczeństwa ISO 27001 lub SOC 2, a magazyn kopii zapasowych musi być zgodny z certyfikatami ISO 9001, ISO 27001 oraz certyfikację DCOS na minimum 4 poziomie.

Funkcje modułu „Zarządzania podatnościami"

1. W skład modułu zarządzania podatnościami Zamawiający wymaga, aby wchodziły następujące funkcjonalności:
   1) Wykrywanie konfiguracji software'owej urządzenia z zainstalowanym Klientem platformy.
   2) Możliwość ręcznego i opartego o harmonogram łatania luk wykrytych przez podstawowe funkcje platformy cyberbezpieczeństwa w kontekście wdrażania poprawek dla systemów operacyjnych urządzeń z zainstalowanym klientem platformy.
   3) Możliwość ręcznego i opartego o harmonogram łatania luk wykrytych przez podstawowe funkcje platformy cyberbezpieczeństwa w kontekście wdrażania poprawek dla aplikacji użytkowych urządzeń z zainstalowanym klientem platformy.
   4) Możliwość wykonania automatycznej kopii zapasowej (awaryjnego punktu powrotu) przed wgraniem poprawek dla luk w kontekście systemu operacyjnego lub aplikacji.
   5) Ocena kondycji pracy urządzenia z klientem platformy bazujące na metodyce ML (Machine Learning) wraz z alarmowaniem o odstępstwa od właściwej pracy oraz możliwością zdefiniowania automatycznych akcji korekcyjnych (np. restart urządzenia czy wykonanie określonego skryptu).Wymagane jest monitorowanie kondycji chronionego urządzenia w minimalnym zakresie: obciążenia procesora oraz procesora graficznego, zajętości i żywotności dysku twardego, wysycenia pamięci RAM, wykorzystania interfejsu sieciowego, temperatury urządzenia, stanu pracy systemowych usług bezpieczeństwa, zmian w konfiguracji sprzętowej i programowej.
   6) Możliwość rozsyłania skryptów PowerShell w sposób zdalny do urządzeń z zainstalowanym klientem platformy.
   7) Repozytorium skryptów z możliwości tworzenie własnych skryptów, w tym możliwość wykorzystania wbudowanych mechanizmów AI do ich tworzenia.
   8) Możliwość rozbudowy typów połączeń zdalnych do urządzeń z klientem platformy o wsparcie dla protokołu zdalnego dostępu, gwarantującego ujednolicony tryb połączenia do urządzeń Windows, Linux oraz macOS.
   9) Możliwość otrzymywania ostrzeżeń o zagrożeniach CyberSecurity z centrum bezpieczeństwa Producenta rozwiązania.

Wymagania dotyczące usług realizowanych przez Wykonawcę:

1. W ramach dostarczenia platformy cyberbezpieczeństwa Wykonawca dokona pełnego wdrożenia rozwiązania w siedzi Zamawiającego, przez co Zamawiający rozumie:

1) Instalacja agentów na wszystkich maszynach wirtualnych oraz stacjach roboczych.
2) Kompleksowa konfiguracja usług bezpieczeństwa platformy, w tym polityk backupu i ochrony.
3) Konfiguracja ma uwzględniać zastosowanie tak zwanych dobrych praktyk dla w/w systemu.
4) Wdrożenie musi obejmować wykonanie kopii zapasowych dla każdego z chronionych w sieci urządzeń, wraz z ich testowym otworzeniem.
5) Wdrożenie musi obejmować konfiguracje między innymi modułu Patch Managment w zakresie wskazanym przez Zamawiającego
6) Wdrożenie musi być wykonane przez osobę posiadającą odpowiednie kompetencje potwierdzone certyfikatami producenta platformy.

W ramach dostarczenia platformy cyberbezpieczeństwa. **Wykonawca przeprowadzi pełne szkolenie z jej funkcjonalności dla działu IT 3 osoby (2 dni robocze po 7 godzin zegarowych z trzema przerwami po 15 minut).**

(3.4) SYSTEM Z FUNKCJĄ DWUETAPOWEGO UWIERZYTELNIENIA WRAZ Z WDROŻENIEM, WSPARCIEM I SZKOLENIEM

Opis Przedmiotu Zamówienia (OPZ)

1. Przedmiot zamówienia

1) Przedmiotem zamówienia jest dostawa oprogramowania wraz z udzieleniem lub zapewnieniem udzielenia licencji przez Wykonawcę Systemu służącego do uwierzytelniania wieloskładnikowego użytkowników.
2) Oferowany System musi istnieć na rynku co najmniej **przez okres 3 lat** oraz posiadać wsparcie techniczne w języku polskim.
3) Producentem Systemu musi być podmiot posiadający siedzibę w Unii Europejskiej.
4) W ramach przedmiotu zamówienia Wykonawca zobowiązuje się udzielić lub zapewnić udzielenie wszelkich licencji wymaganych do prawidłowego działania Systemu, jako całości jak i poszczególnych jego elementów **dla maksymalnie 15 użytkowników, na okres 24 miesięcy** oraz dostarczyć oprogramowanie niezbędne do uruchomienia Systemu.

2. Wymagania ogólne

1) System musi zapewniać konsolę administracyjną dostępną z poziomu przeglądarki internetowej dla administratora w celu konfiguracji i zarządzania.
2) System musi umożliwiać samodzielną rejestrację uwierzytelniaczy (tokenów uwierzytelniających) przez użytkowników.
3) System musi umożliwiać potwierdzenie żądania uwierzytelnienia wieloskładnikowego poprzez zareagowanie na spersonalizowane powiadomienie wysyłane na urządzenie mobilne użytkownika.
4) System musi umożliwiać potwierdzenie żądania uwierzytelnienia wieloskładnikowego poprzez wpisanie kodu jednorazowego pochodzącego z dowolnej aplikacji generującej kody jednorazowe zgodnie ze standardem TOTP (RFC 6238). Przykładami takich aplikacji są Microsoft Authenticator oraz Google Authenticator.
5) System musi umożliwiać potwierdzenie żądania uwierzytelniania wieloskładnikowego poprzez wpisanie kodu jednorazowego wysłanego na numer telefonu użytkownika w postaci wiadomości SMS.
6) System musi wspierać możliwość potwierdzenia żądania uwierzytelnienia wieloskładnikowego poprzez kliknięcie w link wysłany na numer telefonu użytkownika w postaci wiadomości SMS.
7) System musi umożliwiać zebranie zgody użytkownika na wysyłkę wiadomości uwierzytelniających poprzez SMS na numer telefonu użytkownika.
8) System musi umożliwiać wyświetlanie w konsoli administracyjnej informacji o udzielonej zgodzie od użytkownika na wysyłkę wiadomości uwierzytelniających poprzez SMS na wskazany numer telefonu.
9) System musi wspierać możliwość potwierdzenia żądania uwierzytelnienia wieloskładnikowego przy pomocy mobilnej aplikacji uwierzytelniającej, do której dostęp może być zabezpieczony przy pomocy blokady biometrycznej w postaci odcisku palca lub skanu twarzy, jeśli urządzenie mobilne użytkownika posiada taką techniczną możliwość.

10) System musi umożliwiać zakładanie kont administratorów mających dostęp do konsoli administracyjnej wraz z przypisaniem im roli stosownej do zakresu obowiązków danego administratora.
11) System musi umożliwiać identyfikowanie użytkowników po aliasach.
12) System musi umożliwiać udzielanie dostępu do określonych chronionych rozwiązań informatycznych tylko wybranym grupom użytkowników.
13) System musi doprowadzać do wygaśnięcia sesji administratora w konsoli administracyjnej w przypadku nieaktywności administratora.
14) System musi umożliwiać prezentację przeszukiwalnych list zarejestrowanych przez użytkowników numerów telefonów oraz kluczy sprzętowych.
15) System musi zapewnić reguły lub polityki zarządzania żądaniami uwierzytelnienia użytkowników w oparciu o zdefiniowane parametry, takie jak grupa, chroniony zasób, adres IP użytkownika itp.
16) System musi umożliwiać wygenerowanie tymczasowego kodu dostępowego dla wskazanego użytkownika w przypadku niedostępności uwierzytelniacza, np. zagubienia klucza uwierzytelniającego.
17) System musi zapewnić logowanie zapytań uwierzytelniania użytkowników. System musi umożliwiać pobieranie logów w formacie CSV.
18) System musi zapewnić logowanie zdarzeń związanych z obsługą Systemu (wprowadzanie zmian w konfiguracji i politykach, logowanie działań administratorów). System musi umożliwiać pobieranie logów w formacie CSV.
19) System musi posiadać API umożliwiające zarządzanie co najmniej użytkownikami.

3. Wymagane integracje

1) System musi zapewniać możliwość uruchomienia uwierzytelniania wieloskładnikowego dla rozwiązań uwierzytelniających użytkowników ze źródeł Active Directory (LDAP, LDAPS) i RADIUS.
2) System musi zapewniać możliwość wykonywania uwierzytelniania wieloskładnikowego dla systemu operacyjnego Microsoft Windows 10 (i nowszych wersji).
3) System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla technologii Microsoft Outlook Web App (OWA), Microsoft Remote Desktop Gateway/Web Access/Web Client/Web Feed, Microsoft Active Directory Federation Services (AD FS).
4) System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla połączeń przez protokół Remote Desktop Protocol (RDP).
5) System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla połączeń SSH do systemów Linux (Ubuntu 20 i nowszych wersji).
6) System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla dostępu do rozwiązań VPN wykorzystujących co najmniej protokół RADIUS.
7) System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla dostępu do urządzeń sieciowych (routery, switche, zapory sieciowe) wykorzystujące co najmniej protokół RADIUS.
8) System musi umożliwiać integrację z oprogramowaniem własnym poprzez zastosowanie SDK (np. dla oprogramowania .NET, Java, PHP), które umożliwi wykonywanie uwierzytelniania wieloskładnikowego w tym oprogramowaniu.

9) System musi umożliwiać jednostronną synchronizację użytkowników ze źródła Microsoft Active Directory.

4. Wdrożenie

1) Zamawiający wymaga wdrożenia rozwiązania w swojej siedzibie w formie fizycznej obecności Wykonawcy.
2) Wykonawca w ramach wdrożenia dokona niezbędnych aktualizacji obiektów typu „użytkownik" w domenie Zamawiającego w zakresie pól informacyjnych mail oraz numer telefonu przygotowując bazę użytkowników na wdrożenie MFA.
3) Wykonawca w ramach wdrożenia wdroży komponent synchronizujący wybrane grupy użytkowników z serwera Active Directory Zamawiającego z serwerem zarządzania MFA.
4) Wykonawca uruchomi autoryzację dwuetapową dla wszystkich stacji roboczych w środowisku Zamawiającego. W ramach pracy Wykonawca omówi z Zamawiającym stosowną politykę autoryzacji dobierając akceptowane przez Zamawiającego kanały autoryzacji i wyjątki w autoryzacji.
5) Wykonawca uruchomi autoryzację dwuetapową dla połączeń VPN realizowanych w środowisku Zamawiającego. W ramach pracy Wykonawca omówi z Zamawiającym stosowną politykę autoryzacji dobierając akceptowane przez Zamawiającego kanały autoryzacji i wyjątki w autoryzacji.
6) Wykonawca uruchomi autoryzację dwuetapową dla serwerów Windows oraz Linux w kontekście dostępu bezpośredniego (fizyczne logowanie do systemu) oraz zdalnego (RDP oraz SSH). W ramach pracy Wykonawca omówi z Zamawiającym stosowną politykę autoryzacji dobierając akceptowane przez Zamawiającego kanały autoryzacji i wyjątki w autoryzacji.

5. Wykonawca przeprowadzi szkolenie

1) **Szkolenie z działania rozwiązania dla (15 użytkowników) pracowników** Zamawiającego pozwalające pracownikom płynne użytkowanie rozwiązania. Szkolenie musi odbyć się w siedzibie Zamawiającego jednego dnia dla grupy 15 użytkowników x **4 godziny zajęć (godziny zegarowe),** przewiduje się dwie przerwy trwające po 15 minut.
2) **Szkolenie techniczne dla pracowników IT (3 osoby)** Zamawiającego w zakresie zarządzania i administracji rozwiązaniem. Szkolenie musi odbyć się w siedzibie Zamawiającego - c**zas trwania szkolenie 8 godzin (jeden dzień), jednostką czasową szkolenia jest 1 godzina zegarowa, przewiduje się trzy przerwy trwające po 15 minut.**

(3.5) DOSTAWA ZASILACZY AWARYJNYCH (2SZT)

Opis przedmiotu zamówienia (OPZ)

Dostawa dwóch zasilaczy awaryjnych UPS o parametrach identycznych lub lepszych
Opis zasilacza UPS o mocy 5000VA wyposażony w kartę zarządzającą do zasilania:

Tabela 1.1. Minimalne parametry UPS 5kVA

PARAMETR	CECHA/WARTOŚĆ/WŁAŚCIWOŚĆ
Minimalne wymagania techniczne dla jednostki UPS	• Moc znamionowa jednostki nie mniej niż 5000VA / 4500W • Jednostka do montażu w szafie Rack, szyny w zestawie • Technologia Podwójnej konwersji (online) • Klasa VFI-SS-111 zgodnie z PN-EN62040-1 • Temperatura eksploatacji w zakresie 0 - 40 °C • Wilgotność względna podczas pracy w zakresie 0 - 95 % • Hałas słyszalny w odległości 1 m od powierzchni urządzenia max 55dBA • Rozpraszanie ciepła w trybie online ≤1300 BTU/godz. • Sprawność ≥ 94,4% przy pełnym obciążeniu • Klasa ochrony IP 20 • Klasa energetyczna sprzętu przeciwprzepięciowego 480J
Parametry wejściowe	• Nominalne napięcie wejściowe 230VAC • Częstotliwość wejściowa 40–70 Hz (wykrywanie automatyczne) • Typ gniazda wejściowego: Hard wire 3-wire (1P + N + E) • Zmienny zakres napięcia wejściowego w trybie podstawowym 100 – 275VAC (połowa obciążenia), 160 – 275VAC (pełne obciążenie) • Inne napięcia wejściowe 220, 240 (nastawa z wyświetlacza)
Parametry wyjściowe	• Napięcie wyjściowe 230VAC • Zniekształcenia napięcia wyjściowego ≤2% • Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz ± 3Hz • Inne napięcia wyjściowe 220, 240 • Współczynnik szczytu 3: 1 • Typ przebiegu sinusoida • Złącza/gniazda wyjściowe

	Min (6) IEC 320 C13 (Zasilanie gwarantowane) Min (4) IEC 320 C19 (Zasilanie gwarantowane) • Układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny lub ręczny)
Akumulatory i czas podtrzymania	• Typ akumulatora: bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu • Czas autonomii UPS w zestawie z jednym dodatkowym modułem akumulatorowym: min 15 minut dla pełnego obciążenia min 36 minut dla połowy obciążenia • Typowy czas ładowania ≤1,5 godziny • Baterie wymieniane na gorąco • Opcje przedłużonego podtrzymania zasilania: do 10 zewnętrznych modułów bateryjnych, 1 moduł dołączony do UPS
Komunikacja i zarządzanie	• Gniazdo do montażu karty WEB/SNMP • Port uniwersalny do podłączenia np. czujnika temperatury • Porty komunikacyjne: RJ45 Serial, USB • Panel sterowania: LCD - wyświetlacz LCD musi sygnalizować obsłudze stany ostrzegawcze i alarmowe poprzez zmianę koloru podświetlenia ekranu. • Alarmy dźwiękowe i wizualne • Awaryjny wyłącznik zasilania (EPO)
Dodatkowa funkcjonalność	• Zasilacz UPS mus być wyposażony w sterowane programowo gniazda wyjściowe (co najmniej dwie grupy gniazd). Sterowanie gniazd musi umożliwiać sekwencyjne wyłączanie / załączanie odbiorów w zaprogramowanym interwale czasowym. Sterowanie gniazdami musi umożliwiać również powiązanie ze zdarzeniami. • możliwość zimnego startu • automatyczny test akumulatora • automatyczne włączenie UPS-a po powrocie zasilania
Parametry fizyczne	• Maksymalna wysokość 305 mm • Maksymalna szerokość 440 mm • Maksymalna głębokość 720 mm • Wysokość w szafie razem z modułem akumulatorowym – max 7U • Ciężar netto razem z modułem akumulatorowym – max 155 kg • Kolor Czarny

Certyfikaty, zgodności oraz gwarancja	• CE, • **Minimum 36 miesięcy gwarancji producenta** (bez akumulatora) i **24 miesiące gwarancji producenta na akumulatory**
Oprogramowanie	• Dostępne oprogramowanie do zarządzania/monitoringu zgodne z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®.

(3.6) DOSTAWA SERWERA (2SZT)

Opis przedmiotu zamówienia (OPZ)

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. • Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 32 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	• Zainstalowane dwa procesory min. 8-rdzeniowe, taktowane min. 2.9GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 175 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	• Minimum 128GB pamięci RDIMM 4800MT/s, • Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.
Funkcjonalność pamięci RAM	• Demand Scrubing, • Patrol Scrubing, • Permanent Fault Detection

Gniazda PCI	• minimum dwa sloty PCIe generacji 5
Interfejsy sieciowe/FC/SAS	• Wbudowane: – min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT – min. 4 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Dyski twarde	• Zainstalowane 2 dyski SSD M.2 o pojemności min. 480GB w RAID 1
Wbudowane porty	• 4 x USB z czego nie mniej niż 1x USB 3.0, 2x VGA
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	• Redundantne, Hot-Plug min. 1100W każdy.
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 • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku.
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	• **Minimum 36 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu**, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. • 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. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. • Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. • **Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.**

(3.7) DOSTAWA MACIERZY I DOSTAWA 30 SZT DYSKÓW DO MACIERZY kopii offline

Element konfiguracji/cecha /funkcjonalność	Wymagania minimalne
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 4U z możliwością instalacji min. 48 dysków 2.5”
Przestrzeń dyskowa	Zainstalowane dyski: Min. 4x dysk SSD SAS o pojemności min. 1.92TB, Hot-Plug Min. 26 x dysk SAS 10k obr/min. o pojemności min. 2,4 TB
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych.
Obsługa dysków	Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą

	podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać, co najmniej 8 portów 25Gb iSCSI (4 porty na kontroler)
Kable/wkładki	4x kabel DAC 25GbE SFP28/SFP28 min. 2m
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się

	bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.

	Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International)
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. **Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.** Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.

Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:
	• Monitoring:
	  ○ ilość podłączonych oraz rozłączonych systemów
	  ○ stan podłączonych urządzeń

	○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów

	▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie

	operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android

	• Certyfikaty
	  ○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami:
	  ▪ ISO 27001
	  ▪ NIST Security and Privacy Controls for Federal Information Systems and Organization
	  ▪ CSA Cloud Control Matrix

Warunki gwarancji	Zamawiający wymaga zapewnienia gwarancji producenta z zakresu wdrażanej technologii **na okres minimum 36 miesięcy**. **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 Producenta (dla krytycznych zgłoszeń serwisowych) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także 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 Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / 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 Wykonawcy realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.** **Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii.** Charakterystyka usługi diagnostyki: • Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie Zamawiającego. • Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. • Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. • Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. • Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Zamawiającego w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.

	serwis urządzeń będzie realizowany bezpośrednio przez producenta i/lub we współpracy z autoryzowanym partnerem serwisowym producenta. **Firma serwisująca musi posiadać normę ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń**

Dostarczany sprzęt dot. (3.5, 3.6, 3.7) musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w styczniu 2023 r., dostarczony w opakowaniu oryginalnym (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Nie dopuszcza się zastosowania urządzeń tzw. „refurbished".

Zamawiający zastrzega sobie możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów u Producenta, w przypadku wystąpienia wątpliwości co do jego legalności.