1. **Zakup i wdrożenie NAC – 1 szt.**
2. **Testy Bezpieczeństwa – 1 szt.**
3. **Licencja na program do archiwizacji maszyn wirtualnych -1szt.**
4. **Zakup ups-a do szaf PPD - 2 - szt.**
5. **Serwer Archiw – 1 szt.**
6. **Napęd Taśmowy – 1 szt.**

1. Oprogramowanie NAC (Network Access Control) – 1 szt.

1) Minimalna funkcjonalność

Podstawowa funkcjonalność systemu NAC:

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 199 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 300 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
    - VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer
    - Maszyny fizyczne - serwery wspierane przez producenta.
11. System musi posiadać funkcjonalność serwerów:
    - serwera RADIUS dla infrastruktury sieciowej,
    - serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
    - serwera SYSLOG,
    - serwera TACACS+,
    - serwera Monitoringu,
    - serwera DHCP,
    - serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
    - serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.
13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, ODBC.
14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM

MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, ODBC), CheckPoint, Service Now.

16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługi wielu PKI dla różnych grup użytkowników.
20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.
35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
38. System musi posiadać funkcję personalizacji strony gościnnej.

39. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
40. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
41. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
42. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
43. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
45. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
46. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
47. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
48. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
49. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
50. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
51. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
52. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
53. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
54. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
55. System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
56. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
57. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.
58. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
    - Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
    - Czy włączony jest firewall
    - Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
    - Czy jest włączone szyfrowanie dysku systemowego
    - Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
    - Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
    - Czy w systemie są uruchomione procesy wskazane przez administratora
    - Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
    - Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
        - Wartości klucza rejestru

- Typu wartości: Number, String, Version

59. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
60. System musi współpracować z serwerem tokenów.
61. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:
    - Microsoft Windows
    - Mac OS
    - iOS
    - Android
62. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).
63. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

Mechanizmy uwierzytelniania

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
    - MAC,
    - PAP/ASCII,
    - CHAP,
    - SNMP,
    - 802.1X.
3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.
4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
    - Tożsamość/Urządzenie końcowe,
    - Grupa tożsamości/urządzeń końcowych,
    - Parametry urządzeń końcowych, min: system operacyjny, wersja,
    - Atrybuty Active Directory,
    - Jednostka organizacyjna tożsamości/urządzeń końcowych,
    - Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
    - Grupy urządzeń sieciowych,
    - Porty urządzeń sieciowych,
    - Grupy portów urządzeń sieciowych,
    - Jednostka organizacyjna portów,
    - Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
    - Data, czas ważności polityki,
    - Wewnętrzny Captive Portal,
    - Metoda autoryzacji.
8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, MicroTik, Ubiquiti Networks, DCN.

9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
19. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
20. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

Obsługa serwerów certyfikatów CA

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
    - możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
    - możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
    - Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).

Obsługa serwerów DHCP

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
    - Uruchamianie usługi dla wybranych podsieci,
    - Przypisanie ustalonego adresu IP dla adresu MAC.
    - Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
    - Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
    - Możliwość określania braku dostępu dla wybranych adresów MAC,
    - Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
    - Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
    - Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
    - Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
    - Dokonywanie zmian bez konieczności wyłączania usług.

Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.
8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadam adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory, minimum:
    - Logowania, wylogowania z system w tym błędne logowania
    - Logowania do sieci 802.1X

Alarmy

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
    - wiadomości e-mail,

- Syslog,
- notyfikacji systemowych.

2. Alarmy mogą być generowane w sytuacjach, min:
   - Ilości obsługiwanych transakcji RADIUS,
   - Opóźnienie obsługi transkacji RADIUS,
   - Statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
   - badanie łączności IP za pomocą ping, traceroute,
   - tcpdump protokołów RADIUS, TACACS+,
   - wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
     - nazwy użytkownika,
     - adresu MAC,
     - statusu uwierzytelnienia (udana lub nieudana),
     - powodu, jeżeli uwierzytelnienie nieudane,
     - zakresu czasowego, co do dnia, godziny i minuty,
   - wykonanie zdalnego polecenia na urządzeniu sieciowym.

2) Zakres instalacji i konfiguracji
   - Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku Zamawiającego.
   - Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).
   - Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.).
   - Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
   - Integracja urządzeń sieciowych (switche, AP itp.) z systemem NAC (jeżeli urządzenia te wspierają niezbędne funkcjonalności).
   - Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy (jeżeli urządzenia te wspierają niezbędne funkcjonalności).
   - Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.
   - Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia.
   - Wykonawca zapewni 8-godzinne warsztaty w zakresie użytkowania i administrowania wdrożonym systemem NAC.
   - Warsztaty mogą się odbyć w formie zdalnej.
   - Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej.
   - Szczegółowy plan, zakres i termin warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym.
   - Wraz z dożywotnią licencją systemu NAC Wykonawca dostarczy licencję na wsparcie obowiązującą do dnia 09.04.2026 roku, w ramach której Wykonawca zapewni:
     - kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC
     - rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
     - wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.
     - dostęp do dokumentacji i instrukcji na stronie internetowej,
     - dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

2. Zakup systemu do wykonywania testów i badań bezpieczeństwa, kampanii phishingowych oraz testów podatności

1) Wymagania ogólne
   1. System musi posiadać wsparcie techniczne (licencję) do dnia 28.03.2026 r. na niżej opisane funkcjonalności.
   2. System musi umożliwiać wielokrotne przeprowadzenie kampanii phishingowych dla 50 kont poczty elektronicznej.
   3. System musi umożliwiać wielokrotne przeprowadzenie testów podatności 2 (dwóch) stron internetowych.
   4. System musi umożliwiać wielokrotne przeprowadzenie skanowania sieci komputerowej w celu identyfikacji/rozpoznania podłączonych urządzeń.
   5. System musi umożliwiać wielokrotne przeprowadzenie skanowania podatności urządzeń w sieci komputerowej (serwery, przełączniki, dyski NAS, stacje robocze) w ilości 55 szt.
   6. Rozwiązanie typu manager/konsola ma musi być dostępne w chmurowej (SaaS).
   7. Rozwiązanie musi posiadać swoje centrum danych (data center) na terenie Unii Europejskiej.
   8. Rozwiązanie musi oferować możliwość wdrożenia sond skanujących w postaci gotowych maszyn wirtualnych, które muszą być udostępnione w postaci obrazu maszyny OVA lub dysku VHDX.
   9. Sonda skanująca musi wymagać rejestracji, w konsoli centralnej Security Center, przy użyciu wygenerowanego przez administratora sześcioznakowego tokena lub innego mechanizmu uwierzytelniania.
   10. Konsola centralna musi posiadać możliwość uruchomienia dodatkowego uwierzytelnienia użytkowników, za pomocą 2FA wysyłanych w postaci wiadomości SMS.
   11. Administrator w konsoli centralnej musi posiadać możliwość dodania dodatkowych użytkowników zarządzających.
   12. Rozwiązanie musi posiadać możliwość dodania dodatkowych zestawów uprawnień (ról), które mogą być przypisane do użytkowników systemu.

2) Zarządzanie zestawami
   1. Rozwiązanie musi posiadać możliwość dodania ręcznego urządzeń i aplikacji webowych do skanowania.
   2. Rozwiązanie musi posiadać możliwość importu listy urządzeń z pliku CSV.
   3. Dodanie urządzeń musi odbywać się za pomocą podania pojedynczego adresu IP, zakresu adresów IP oraz adresu sieci wraz z maską.
   4. Dodanie aplikacji webowej musi pozwalać na dodanie rodzaju autentykacji, białej i czarnej listy adresów URL oraz rozszerzeń do skanowania.
   5. Przy dodawaniu urządzeń i aplikacji webowych administrator musi posiadać możliwość wyboru poziomu wpływu biznesowego z jednego z 4 poziomów: Neutralny, Niski, Średni i Wysoki (nazewnictwo przykładowe).
   6. Przy dodawaniu urządzeń i aplikacji webowych administrator musi posiadać możliwość wyboru znaczników (tagów).
   7. Administrator musi posiadać możliwość dodania znaczników (tagów) dynamicznych, które będą przypisywane do urządzeń po spełnieniu jednego z warunków: nazwy zestawu urządzeń, adresu IP z podanego zakresu, otwartych portów lub systemu operacyjnego.

3) Skanowanie sieciowe

   1. Rozwiązanie musi posiadać możliwość zapewnienia nieograniczonej liczby skanów i nieograniczonej liczby zaplanowanych skanów oraz skanów na żądanie. Powiadomienia powinny być również dostępne za pośrednictwem integracji e-mail.

2. Rozwiązanie musi posiadać możliwość skanowania całego środowiska IT z segmentowanymi i geograficznie oddzielonymi sieciami.
3. Usługa skanowania sieci musi obsługiwać IPv6.
4. Rozwiązanie musi posiadać możliwość dodawania różnych profili skanowania sieciowego.
5. Administrator musi posiadać możliwość importu predefiniowanych przez producenta profili skanowania sieciowego.
6. Funkcja wykrywania urządzeń w profilu skanowania, musi pozwalać na wybór domyślnych portów, dodanie dodatkowych portów, wybór rodzaju połączenia TCP SYN lub TCP SYN ACK oraz możliwość wyłączenia lub włączenia wysłania ICMP PING.
7. Rozwiązanie musi posiadać możliwość uwzględnienia podatności o niskim prawdopodobieństwie wystąpienia w wynikach skanowania.
8. Rozwiązanie musi umożliwiać włączenia skanowania drukarek.
9. Rozwiązanie musi posiadać możliwość uwzględnienia martwych hostów w skanach.
10. Możliwość włączenia opcji - brutalnego wymuszania hasła - do ustawień skanowania.
11. Profil skanowania sieciowego musi posiadać możliwość dodania uwierzytelniania na urządzeniu sieciowym, w oparciu o uwierzytelnianie Windows i/lub Linux.
12. Profil skanowania sieciowego musi posiadać możliwość wyboru intensywność skanowania.
13. Profil skanowanie sieciowego musi posiadać możliwość wyboru testów podatności, które będą przeprowadzone w trakcie skanowania.
14. Rozwiązanie musi posiadać co najmniej 100 tys. testów podatności aktualizowanych na bieżąco z serwera producenta rozwiązania.
15. Podczas tworzenia zadania skanowania sieciowego, administrator musi posiadać możliwość wyboru sondy skanującej zainstalowanej lokalnie, grupy sond lub sondy zewnętrznej hostowanej w chmurze producenta.
16. Administrator musi posiadać możliwość uruchomienia zadania skanowania sieci jednorazowo lub z harmonogramem.
17. Urządzenia znalezione podczas zadania skanowania muszą zostać automatycznie dodane do listy urządzeń wraz z odpowiednimi znacznikami (tagami), przypisanymi na podstawie wykrytych portów usług oraz systemu operacyjnego.
18. Podatności wykryte podczas skanowania sieciowego muszą automatycznie być umieszczane w menedżerze podatności.

4) Skanowanie aplikacji webowych

1. Rozwiązanie musi posiadać możliwość dodawania nowych profili skanowania aplikacji webowych.
2. Administrator musi posiadać możliwość importu predefiniowanych przez producenta profili skanowania aplikacji webowych.
3. Rozwiązanie musi posiadać możliwość skanowania aplikacji internetowych (skanowanie stron internetowych).
4. Rozwiązanie musi posiadać możliwość zapewnienia nieograniczonej liczby skanów i nieograniczonej liczby zaplanowanych skanów oraz skanów na żądanie. Powiadomienia powinny być również dostępne za pośrednictwem integracji e-mail.
5. Rozwiązanie musi posiadać możliwość zapewnienia konfigurowalnych ustawień skanowania, takich jak ustawienia indeksowania do metody formularza: Post i Get, Post, Get.
6. Podczas tworzenia zadania skanowania aplikacji webowych, administrator musi posiadać możliwość wyboru sondy skanującej zainstalowanej lokalnie lub sondy zewnętrznej hostowanej w chmurze producenta.
7. Podczas tworzenia profilu skanowania aplikacji webowych administrator musi posiadać możliwość włączenia i wyłączenia wykonania testów „łamania” haseł typu brute force.

8. Rozwiązanie musi posiadać możliwość wyboru intensywności skanowania wydajności (wstępnie ustawiona na niską, średnią i wysoką) przez system.
9. Rozwiązanie musi posiadać możliwość włączenia pełnego zestawu kategorii wykrywania podatności, a także dostosowania kategorii wykrywania podatności do skanowania, a także listy wykluczeń.
10. Rozwiązanie musi posiadać możliwość wyboru opcji skanowania wrażliwych treści, numerów kart kredytowych i zezwalania na wprowadzanie niestandardowych treści.
11. Administrator musi posiadać możliwość uruchomienia zadania skanowania aplikacji webowej jednorazowo lub z harmonogramem.
12. Podatności wykryte podczas skanowania aplikacji webowych muszą automatycznie być umieszczane w menedżerze podatności.

5) Skanowanie agentowe

1. Rozwiązanie musi posiadać możliwość instalacji na systemach Windows aplikacji agentowej, która będzie przesyłać do konsoli centralnej listę zainstalowanych aplikacji.
2. Systemu musi posiadać bazę podatności aplikacji zainstalowanych w systemach skanowanych przez aplikację agentową.
3. Wykryte przez aplikację agentową podatności muszą automatycznie być umieszczane w menedżerze podatności.
4. Pakiet instalacyjny aplikacji agentowej musi być udostępniony w postaci pliku .msi.
5. Aktywacja aplikacji agentowej musi wymagać podania, wygenerowanego w konsoli centralnej, tokenu lub innej informacji uwierzytelniającej.

6) Zarządzanie aktywami

1. Rozwiązanie musi posiadać możliwość wyświetlenia listy zeskanowanych zasobów: adres IP sieci i aplikacje internetowe z następującymi informacjami:
    a. Oznaczanie (lista grupowania)
    b. Nazwa zasobu
    c. Liczba wykrytych podatności w zabezpieczeniach
    d. Najwyższa wykryta podatność
    e. Krytyczność/istotność dla Zamawiającego
    f. Informacje o systemie operacyjnym
    g. Data wprowadzenia utworzonych zasobów i ostatnio wykryty znacznik czasu
2. Rozwiązanie musi posiadać możliwość przeglądania informacji o aktywach, takich jak:
    a. Sieć: Stan podatności - Aktywne, Ignorowane i Wyłączone.
    b. Sieć : Status podatności - Nowa, Aktywna, Ponownie otwarta i Naprawiona
    c. Sieć: lista otwartych portów powiązanych z zasobem
    d. Sieć: Trend zasobu - według ważności, stanu. Możliwość wyświetlania według okresu i przedziału czasu.
    e. Aplikacja internetowa : Stan podatności - Aktywne, Ignorowane i Wyłączone.
    f. Aplikacja internetowa : Status podatności - Nowa, Aktywna, Ponownie otwarta i Naprawiona
    g. Aplikacja internetowa : Lista przeskanowanych i wykrytych map witryn
    h. Aplikacja webowa: Trend zasobu - według ważności, stanu. Możliwość wyświetlania według okresu i interwału.
3. Potrafi zapewnić możliwość edycji informacji o aktywach, takich jak:
    a. Sieć: Aby podać nazwę zasobu (jeśli nie jest dostępny DNS).
    b. Sieć: aby podać etykietę wpływu biznesowego
    c. Sieć: Aby podać kolumnę wejściową dla opisu zasobu
    d. Sieć: możliwość wybrania, czy zasób przechowuje jakiekolwiek dane osobowe RODO
    e. Aplikacja internetowa: Aby podać nazwę zasobu

f. Aplikacja internetowa: Aby podać etykietę wpływu biznesowego
g. Aplikacja internetowa: Aby zapewnić kolumnę wejściową dla opisu zasobu
h. Aplikacja internetowa: Rozwiązanie musi posiadać możliwość wybrania, czy zasób przechowuje jakiekolwiek dane osobowe RODO
i. Aplikacja internetowa: Rozwiązanie musi posiadać możliwość zapewnienia funkcji skanowania REST API
j. Aplikacja internetowa: Może zapewnić zakres indeksowania, taki jak nazwa hosta adresu URL i podkatalog adresu URL. A także w stanie jawnie określić inne adresy URL
k. Aplikacja webowa: Możliwość podawania nagłówków i plików cookie
l. Aplikacja internetowa: może zapewnić uwierzytelnione skanowanie, takie jak HTTP Basic i HTTP Form
m. Aplikacja internetowa: Może zapewnić elastyczność w utrzymywaniu listy wykluczających adresów URL, takich jak biała i czarna lista.
n. Aplikacja internetowa: Rozwiązanie musi posiadać możliwość wyświetlenia listy zeskanowanych luk w zabezpieczeniach powiązanych z zasobami aplikacji internetowej.

4. Rozwiązanie musi potrafić zapewnić funkcje tworzenia i utrzymywania tagów (grup) statycznych i dynamicznych.
5. Rozwiązanie musi posiadać możliwość tworzenia ręcznego wprowadzania i importowania zasobów kategorii Network IP

7) Moduł kampanii phishingowych
1. Rozwiązanie musi posiadać możliwość utworzenia kampanii phishingowej i edukacyjnej.
2. Administrator musi posiadać możliwość utworzenia własnych profili phishingowych lub importu predefiniowanych przez producenta.
3. Profile kampanii phishingowych utworzone przez producenta muszą być dostępne w języku polskim.
4. Profil kampanii phishingowej powinien zawierać szablon wiadomości email lub wiadomości email i strony internetowej.
5. Rozwiązanie musi posiadać możliwość przypisania do profilu kampanii phishingowej kategorii domen, z których wysyłane będą wiadomości.
6. Kampanie phishingowe muszą posiadać możliwość wyboru czasu rozpoczęcia kampanii oraz czy wiadomości mają być wysyłane jednorazowo do wszystkich odbiorców, w grupach lub losowo w określonym zakresie czasu.
7. Platforma musi posiadać co najmniej 5 predefiniowanych szablonów kampanii:
   a. Polski: Wiadomości phishingowe - oszustwo związane z kontem e-mail
   b. Polski: Wiadomości phishingowe i strony internetowe - oszustwa związane z kontami e-mail
   c. Polski: Wiadomości phishingowe i strony internetowe - oszustwa związane z kartami kredytowymi
   d. Polski: Pobieranie plików - Office 365
   e. Polski: Phishing - Office 365

8. Administrator musi posiadać możliwość przypisania do kampanii phishingowej, kampanii edukacyjnej przeprowadzanej poprzez wysłanie wiadomości email i/lub strony internetowej.
9. Administrator musi posiadać możliwość utworzenia własnych profili edukacyjnych lub importu predefiniowanych przez producenta.
10. Profile kampanii edukacyjnych utworzone przez producenta muszą być dostępne w języku polskim i angielskim.
11. Rozwiązanie musi posiadać możliwość wyboru treści wiadomości edukacyjnej w zależności od podjętej przez odbiorcę czynności: otwarcia wiadomości, odpowiedzi na wiadomość, kliknięcia w link oraz wypełnienia formularza na stronie phishingowej.

12. Rozwiązanie musi posiadać możliwość stworzenia oraz wyboru treści prezentacji edukacyjnej w formie strony internetowej na której można zamieszczać treści edukacyjne w postaci tekstu, grafiki oraz wideo.
13. Rozwiązanie musi posiadać możliwość stworzenia oraz wyboru testu sprawdzającego wiedzę w formie strony internetowej na której można zamieszczać pytania i odpowiedzi w formie jednokrotnego i wielokrotnego wyboru.
14. Rozwiązanie musi posiadać możliwość anonimizacji danych odbiorców i podjętych przez nich czynności.

8) Menadżer podatności

1. Platforma zarządzania podatnościami musi być w stanie zapewnić funkcje pulpitu nawigacyjnego (i konfigurowalne) z następującymi widżetami:
    a. Wyniki skanowania podatności sieci według ważności (z opcjami wykresów)
    b. Wyniki skanowania podatności aplikacji internetowych według ważności (z opcjami wykresów)
    c. Otwarte zgłoszenia według ważności (z opcjami wykresów)
    d. Top 10 wyników skanowania sieci (dostępna opcja ustawienia celu zasobu jako wszystkich lub wybranych adresów IP / tagów)
    e. 10 największych podatności w aplikacjach sieciowych (dostępna opcja ustawienia celu zasobu jako wszystkie lub wybrane aplikacje sieciowe/etykiety)
    f. Zgodność z OWASP (z opcjami wykresów : Słupkowy i kołowy oraz dostępną opcją ustawienia dla wszystkich lub wybranych aplikacji internetowych)
    g. Ostatnie skanowania
    h. Nadchodzące skanowania
    i. Ostatnie 10 raportów
    j. Liczba podatności w zabezpieczeniach w czasie (dostępna opcja ustawienia celu zasobu jako wszystkich lub wybranych aplikacji Ips / Web / tagów wraz z ustawieniem czasu, aby ustawić czas trwania i interwał)
    k. Ocena wyników kampanii phishingowych
    l. Ciągłe monitorowanie alertów (dostępna opcja ustawienia okresu na dzień/tydzień)
2. Platforma zarządzania podatnościami musi mieć możliwość sortowania, grupowania i priorytetyzacji podatności
    a. Możliwość tworzenia wielu zakładek w celu filtrowania następujących kryteriów:
    b. Według stanu : Wszystkie, Nie ignorowane/wyłączone i ignorowane/wyłączone.
    c. Według typu: Host i aplikacja internetowa
    d. Według statusu : Nowy, Aktywny, Ponownie otwarty, Naprawiony
    e. Według ważności : Informacja, Niski, Średni, Wysoki, Krytyczny
    f. Według tagów (opcja uwzględnienia/wykluczenia tagu)
    g. Według pierwszego i ostatniego wykrycia
    h. Według kategorii: podatności w skanowaniu sieci i podatności w aplikacjach internetowych
    i. Możliwość filtrowania listy podatności według podatności lub aplikacji internetowych / hosta.
    j. Możliwość tworzenia raportów bezpośrednio z Menedżera podatności poprzez wybranie jednej lub więcej podatności.
    k. Możliwość dalszego administrowania / zarządzania listą luk w zabezpieczeniach za pomocą następujących funkcji:
    l. Co ignorować: Wyłącz tę podatność dla wszystkich hostów/aplikacji internetowych i Ignoruj tę podatność.
    m. Powód ignorowania : Fałszywie dodatni, Ryzyko zaakceptowane, Nieistotne
    n. Opcja ustawienia czasu wygaśnięcia dla ignorowanych podatności

   o. Możliwość tworzenia notatek do celów uwag i notatek, które pojawią się w raporcie po jego wygenerowaniu
   p. Możliwość tworzenia czatu konwersacyjnego do celów współpracy między użytkownikami
   q. Opcja wyświetlania następujących informacji na temat podatności -
      i. Wpływ
      ii. Rozwiązanie
      iii. Podsumowanie
      iv. Wgląd
      v. Wykrywanie
      vi. Odniesienie
      vii. Łatki
      viii. Możliwość utworzenia zgłoszenia bezpośrednio ze wskazanych luk w zabezpieczeniach
      ix. Środki zaradcze
3. Możliwość dostarczania informacji o zgłoszeniach, takich jak:
   a. Numerowanie ich w celu łatwego śledzenia i powiadamiania za pośrednictwem poczty elektronicznej.
   b. Możliwość podawania i aktualizowania statusu zgłoszenia, takiego jak : Otwarte, Zamknięte lub Rozwiązane
   c. Możliwość podania nazwy powiązanej podatności w zabezpieczeniach wraz z jej zasobami
   d. Możliwość podania wagi podatności w zabezpieczeniach zarejestrowanego zgłoszenia
   e. Możliwość przypisania do wyznaczonego właściciela i terminu płatności
   f. Możliwość tworzenia wielu zakładek do utrzymywania i zarządzania zgłoszeniami zgodnie z poniższymi zasadami:
   g. Status
   h. Typ zasobu
   i. Kategoria usługi
   j. Tagi
   k. Termin płatności
   l. Kategoria skanowania sieci i aplikacji internetowych
   m. Istotność
   n. System operacyjny
   o. Porty
   p. Właściciel
   q. Potrafi zapewnić proaktywną obsługę zgłoszeń opartą na zasadach
4. Rozwiązanie musi posiadać możliwość ciągłego monitorowania oraz szybkiego i łatwego ustawienia profilu monitorowania zmian za pomocą powiadomień i alarmów.
5. W menedżerze podatności musi istnieć możliwość utworzenia własnego widoku podatności zawierającego odfiltrowane zgodnie z konfiguracją administratora danych.
6. Rozwiązanie musi posiadać możliwość zignorowania wykrytych podatności na określony czas.

9) System raportujący

System raportujący musi zawierać następujące raporty:

7. Skanowanie sieci
8. Aplikacja sieciowa
9. Łatki
10. Środki zaradcze
11. Ocena phishingu e-mail
12. Porównanie (raport Delta)
13. Zgodność
14. Raporty zgodności: Musi być w stanie wygenerować następujący typ zgodności:

   a. Ustawa o ochronie danych osobowych
   b. ISO / IEC 27001
   c. Ogólne rozporządzenie o ochronie danych
   d. Bezpieczeństwo sieci i informacji
15. System powinien mieć możliwość dostarczania nowych niestandardowych raportów zgodności, które mogą być zalecane przez rząd, gdy ma to zastosowanie.
16. Rozwiązanie musi posiadać możliwość tworzenia i dostosowywania szablonów raportów sieciowych z następującymi opcjami:
   a. Raport oparty na określonym czasie skanowania
   b. Raport oparty na wszystkich bieżących informacjach o podatnościach
   c. Raport trendów z historią podatności
   d. Zawartość raportu : Szczegóły raportu, przegląd podatności, podsumowanie podatności, lista podatności (według podatności i hosta) z opcjami wglądu, podsumowania, wykrywania, odniesień i ograniczenia tekstu do 500 znaków.
   e. Sposób prezentacji raportu: Podatności według ważności w czasie, Podatności według statusu, Podatności według ważności, 5 najbardziej narażonych kategorii
   f. Filtrowanie: Selektywne raportowanie podatności (pełne i niestandardowe) i wykluczenia, Uwzględnione systemy operacyjne, Filtry zasobów, Filtry podatności
17. Potrafi utworzyć i dostosować szablon raportu aplikacji internetowej z następującymi opcjami:
18. Raport oparty na określonym czasie skanowania
19. Raport oparty na wszystkich bieżących informacjach o podatnościach
20. Filtrowanie: Selektywne raportowanie podatności (pełne i niestandardowe) i wykluczenia, Uwzględnione systemy operacyjne, Filtry zasobów, Filtry podatności
21. Możliwość tworzenia "raportów skróconych" wysyłanych w sposób podsumowujący. Częstotliwość raportów można ustawić na: tygodniowe raporty skrócone i miesięczne raporty skrócone. Raporty mają byc dostarczane kanałem e-mail.

3. Program do archiwizacji danych i maszyn wirtualnych

Wymagania ogólne

- Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x i 8.0 oraz Microsoft Hyper-V 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
- Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
- Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
- Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie jest wymagana osobna baza danych z metadanymi deduplikowanych bloków.
- Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
- Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
- Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe.
- Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage.
- Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
- Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.
- Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
- Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
- Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.
- Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
- Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.
- Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora).
- Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS).
- Oprogramowanie musi posiadać integracje z systemami typu SIEM.
- Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
- Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
- Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru.
- Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO).
- Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
- Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
- Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
- Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.
- Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).
- Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
- Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej

na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk Vmware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.

- Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
- Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
- Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.
- Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
- Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux.
- Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM.
- Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
- Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites.
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
- Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
- Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI.
- Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
- Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.
- Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender oraz ESET.
- Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware.
- Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania.
- Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
- Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
- Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
- Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, CentOS.
- Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux.
- Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą).
- Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster.
- Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów.
- Rozwiązanie musi wspierać backup podłączonych dysków USB.
- Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym.
- Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury).

- Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone.
- Rozwiązanie musi wspierać kontrolę pasma sieciowego.
- Rozwiązanie musi wspierać technologię BitLocker.
- Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania.
- Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych.
- Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle i PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
- Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V.
- Rozwiązanie musi wspierać szyfrowanie.
- Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego.
- Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej.
- Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.
- System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich.
- System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
- System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
- System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
- System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej.
- System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.
- System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
- System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
- System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, PDF.
- System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.
- System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.
- System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.
- System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.
- System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
- System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
- System musi być objęty licencją wieczystą na backup minium 5 maszyn wirtualnych z 2 letnim wsparciem producenta.

4. Zakup ups-a do szaf PPD

Parametr	Charakterystyka (wymagania minimalne)
Technologia	online, VFI-SS-111,
Moc wyjściowa	3kVA/3kW; PF=1
Obudowa	Rack/Tower Zestaw do montażu w szafie rack na wyposażeniu
Napięcie wejściowe	110 ÷ 300 V AC ± 2 %
Napięcie znamionowe (wartość skuteczna)	230V AC
Prąd znamionowy (wejście)	15,6A
Częstotliwość napięcia wejściowego (zakres oraz tolerancja)	45 ÷ 55 / 55 ÷ 65 Hz ± 1 Hz
Częstotliwość znamionowa napięcia wejściowego	50Hz / 60Hz
Zniekształcenia prądu wejściowego THDi	< 5%
Zakres napięcia wyjściowego	200/208/220/230/240V AC konfigurowalne z poziomu oprogramowania oraz z menu zasilacza na wyświetlaczu LCD (domyślnie 230V AC
Zniekształcenia napięcia wyjściowego THDu	< 1% dla Pmax (liniowe) < 5% (nieliniowe wg PN EN 62040-3)
Gniazda wyjściowe	4x IEC320 C13 (10A) sterowalne + 4x IEC320 C13 (10A) + 1x IEC320 C19 (16A)
Akumulatory wewnętrzne UPS	Minimum 6szt akumulatorów 12V9Ah
Moduły bateryjne	Opcja – możliwość podpięcia do 4szt modułów (każdy z minimum 12szt akumulatorów 12V9Ah)
Czas podtrzymania UPS dla obciążenia 3kW/2,4kW/1,5kW	3,5 / 5 / 10 min

Przeciążalność	105-125% - 5min / 125-150% - 30s / >150% - 500ms
EPO	Wymagane – standard NC
Sygnalizacja	akustyczno-diodowa, wyświetlacz LCD oraz diody sygnalizujące usterkę, pracę bateryjną, pracę w trybie online, obejście bypass
Język oprogramowania	polski i angielski do wyboru z poziomu interfejsu użytkownika
Konfiguracja minimalnego poziomu naładowania baterii po powrocie zasilania sieciowego (po rozładowaniu baterii przed ponownym samoczynnym załączeniem zasilania na wyjściu)	Wymagane, konfigurowalne z poziomu oprogramowania (przez USB)
Wymagane certyfikaty	CE, ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu; (załączyć dokument)
Komunikacja z urządzeniem	RS232, USB HID, styki bezpotencjałowe 1-wejście; 1-wyjście; SNMP – Karta w zestawie.
Oprogramowanie do monitorowania pracy zasilacza UPS	Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na min. 75 stanowiskach komputerowych w sieci; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów (potwierdzone oświadczeniem producenta oprogramowania)
Oprogramowanie - funkcjonalność	możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPS'ów w oprogramowaniu
Oprogramowanie - funkcjonalność	Konfiguracja minimalnego poziomu naładowania baterii. UPS po rozładowaniu baterii przed samoczynnym załączeniem zasilania wyjść (po powrocie zasilania sieciowego) będzie musiał naładować baterie do tego poziomu. Parametr ten ma zastosowanie w przypadku, gdy załączenie zasilania wyjść może nastąpić tylko wtedy, gdy UPS zgromadzi niezbędny zapasa energii na wypadek kolejnego zaniku.
Oprogramowanie - funkcjonalność	Uruchom poprzez Bypass - Aktywacja tej funkcji powoduje, że UPS zawsze przed załączeniem zasilania wyjść na kilka sekund załączy zasilanie poprzez Bypass i po chwili przełączy się w zasilanie wyjść poprzez falownik (normalny tryb pracy). Funkcja ta umożliwia załączenie urządzeń o zwiększonym prądzie rozruchowym bez przeciążania falownika UPS.
Serwis producenta	wymagany, zlokalizowany na terenie Polski, autoryzacja serwisowa lub oświadczenie producenta - załączyć do oferty
Gwarancja	Minimum 24 miesiące elektronika, 24 miesiące akumulatory
Dokumentacja	Instrukcja w języku polskim

5. Serwer kopii zapasowych

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. • Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. • Obsługa procesorów 8 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Płyta główna powinna obsługiwać do 128GB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych.
Procesor	• Zainstalowany jeden procesor min. 8-rdzeniowy, min. 2.6 GHz, dedykowany do pracy z zaoferowanym serwerem, umożliwiający osiągnięcie wyniku min 84.4 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla oferowanego modelu serwera wyposażonego w jeden procesor.
RAM	• Minimum 64GB DDR5 UDIMM 5600MT/s • Na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone do instalacji pamięci.
Gniazda PCI	• minimum dwa sloty PCIe x8 generacji 4
Interfejsy sieciowe/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT • Dodatkowa karta SAS umożliwiająca połączenie z napędem taśmowym
Dyski twarde	• Możliwość instalacji dysków SATA, SAS, SSD • **Zainstalowane 3 dyski HDD SAS o pojemności min. 1.2TB, 12Gbps, 2,5“ Hot-Plug.** • **Zainstalowane 2 dyski M.2 NVMe o pojemności min. 480GB z możliwością konfiguracji RAID 1.**

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

Wbudowane porty	• 3 x USB z czego nie mniej niż 1x USB 3.0, 1x VGA
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	• Redundantne, Hot-Plug min. 700W każdy, klasy Titanium • min. 2 kable zasilające typu C13/C14 o długości min. 2 metry
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
System operacyjny	• Zakres Przedmiotu Zamówienia obejmuje dostarczenie Serwerowego Systemu Operacyjnego, zwanego dalej SSO. • Licencja musi uprawniać do uruchamiania min. **dwóch** wystąpień SSO, w środowisku fizycznym i wirtualnym lub wyłącznie wirtualnym za pomocą wbudowanych mechanizmów wirtualizacji. • SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, d) 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, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: 1. pozwalają na zmianę rozmiaru w czasie pracy systemu, 2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, 3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, 4. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, q) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), r) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, s) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, t) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: 1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 2. 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 SSO 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, 3. zdalna dystrybucja oprogramowania na stacje robocze, 4. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, 5. 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, 6. szyfrowanie plików i folderów, 7. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), 8. możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów, 9. serwis udostępniania stron WWW, 10. wsparcie dla protokołu IP w wersji 6 (IPv6), 11. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 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 model), u) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, v) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), w) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, x) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, y) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej; o 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 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)
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-14001:2015 oraz ISO-50001:2018 • Serwer musi posiadać deklarację 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 - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
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 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. • Możliwość odpłatnego przedłużenia gwarancji producenta do 7 lat. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

	• Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera

6. Napęd LTO

Element konfiguracji	Wymagane minimalne parametry techniczne
Wykorzystana Technologia	LTO Ultrium wspierające technologię partycjonowania nośników. Urządzenie powinno mieć możliwość instalowania w tej samej obudowie także napędów LTO szóstej, siódmej i dziewiątej generacji
Wbudowany napęd	Napęd LTO-8 wyposażony w złącze SAS 6Gb. Oferowane urządzenie musi mieć możliwość instalowania i wykorzystania w tej samej obudowie także napędów LTO z interfejsem FC oraz wspierać technologię LTFS (Linear Tape File System). Prędkość zapisu zainstalowanego napędu bez kompresji – minimum 300 MB/sek. Zainstalowany napęd musi dynamicznie i płynnie dopasowywać prędkość zapisu do napływających danych (speed matching) w przedziale od 100 do 300 MB/sek., oferować funkcję SkipSync zapewniającą dużą szybkość zapisu małych plików bez konieczności zatrzymywania i przewijania dysku oraz stosować szyfrowanie danych metodą AES 256-bit zgodną ze standardem FIPS 140-2
Ilość slotów i magazynki	Minimalnie 8 slotów na nośniki podzielone na dwa magazynki – dwa magazynki są wymagane w celu szybszego dojścia do danych i prostszego zarzadzania nośnikami i szybszej ich weryfikacji. Urządzenie powinno być dostarczone z kompletem magazynków. Wymagana ilość mail slot (I/E): 1. Możliwość zdalnego wysuwania magazynków poprzez web GUI
Pojemność	Pojemność bez kompresji – minimum 96TB
Zarządzanie	Za pomocą panelu kontrolnego znajdującego się na froncie urządzenia oraz zdalne przez sieć poprzez przeglądarkę internetową (web GUI) za pomocą interfejsu FastEthernet. Wymagane wsparcie SNTP, protokołów SSL/TLS i IPv6 oraz definiowanie minimum 4 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji na podłączony, poprzez slot USB, PenDrive. Operacja powinna być możliwa zarówna poprzez web GUI jak i poprzez panel kontrolny urządzenia. Wymagana możliwość zdalnego wysuwania magazynków, restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI.
Dodatkowe interfejsy	Biblioteka musi być wyposażone w interfejs sieciowy, interfejs USB oraz interfejs ADI
Obsługa urządzenia	Możliwość wymiany napędu, zasilacza i modułu portów zarządzania u użytkownika bez konieczności demontażu urządzenia z szafy przemysłowej oraz bez konieczności zdejmowania pokrywy głównej. Zarówno napęd jaki moduł interfejsów powinny być wyposażone w lamki kontrolne, informujące o stanie technicznym i widoczne na odwrotnej stronie urządzenia.
Obudowa	Typu rack 19” o wysokości maksymalnie 1U. Wszystkie elementy do montażu muszą być dostarczone wraz z urządzeniem
Wyposażenie	Urządzenie musi być wyposażone w czytnik kodów kreskowych, kabel zasilający, kabel komunikacyjny konieczny do podłączenia urządzenia do odpowiedniego kontrolera serwera i umożliwiającego komunikację z urządzeniem – długość kabla min. 2m (w przypadku, gdyby serwer backupu nie dysponował odpowiednim kontrolerem, należy taki dostarczyć wraz z urządzeniem – interfejs kontrolera: minimum dual SAS 12Gb), zestaw 10 nośników danych o pojemności bez kompresji minimum 12 TB każdy wraz z nośnikiem czyszczącym, przy czym wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem. Kompatybilność nośników taśmowych z urządzeniem musi zostać potwierdzona przez oświadczenie producenta dostarczone wraz z ofertą.
Gwarancja i oświadczenia	60 miesięcy w miejscu instalacji urządzenia z czasem reakcji serwisu na zgłoszenia w ciągu 8 godzin. Czas przyjmowania zgłoszeń serwisowych w trybie 5x9. Przystąpienie do fizycznej naprawy najpóźniej w następnym dniu roboczym od zgłoszenia awarii z terminem naprawy najpóźniej do 48 godzin od rozpoczęcia naprawy. Gwarantowana możliwość rozszerzenia oferowanego serwisu do 84 miesięcy. Zgłaszania awarii wyłącznie poprzez ogólnopolską linię telefoniczną producenta lub autoryzowanego serwisu producenta posiadającego certyfikat ISO9001 na usługi serwisowe – kontakt z serwisem wyłącznie w języku polskim. Pisemne oświadczenia wystawione przez producenta:

	- o gwarancji świadczonej w miejscu instalacji urządzenia w rygorze 5x9x8 realizowanej przez producenta lub jego autoryzowany serwis posiadający ISO9001 na usługi serwisowe wraz z potwierdzeniem możliwości przedłużenia gwarancji do 84 miesięcy. W oświadczeniu wymagane jest podanie wszystkich danych kontaktowych z serwisem (mail, telefon, adres)