**OPIS PRZEDMIOTU ZAMÓWIENIA**

Spis treści

[CZĘŚĆ I – Przegląd i aktualizacja dokumentacji SZBI oraz audyt końcowy bezpieczeństwa informacji Urzędzie Gminy 2](#_Toc215733085)

[CZĘŚĆ II – Przeprowadzenie szkoleń nt. bezpieczeństwa informacji dla pracowników Urzędu w ramach realizacji grantu Cyberbezpieczny Samorząd 4](#_Toc215733086)

[1. Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników Urzędu Gminy 4](#_Toc215733087)

[2. Przeprowadzenie szkoleń specjalistycznych dla Informatyka Urzędu w dziedzinie technologii i cyberbezpieczeństwa 6](#_Toc215733088)

[CZĘŚĆ III - Dostawa urządzeń i oprogramowania zwiększających odporność na cyberataki wraz z wdrożeniem 8](#_Toc215733089)

[1. UTM – 1 szt. 9](#_Toc215733090)

[2. Przełączniki sieciowe Typ 1 – 2 szt. 16](#_Toc215733091)

[3. Przełączniki sieciowe Typ 2 – 6 szt. 18](#_Toc215733092)

[4. Przełącznik sieciowy typ 3 – 1 szt. 20](#_Toc215733093)

[5. Przełączniki sieciowe typ 4 – 2 szt. 22](#_Toc215733094)

[6. Agregat 24](#_Toc215733095)

[7. Zasilacz UPS stanowiskowy – typ 1 – 54 szt. 28](#_Toc215733096)

[8. Zasilacz UPS - Typ 2 – 2 szt. 30](#_Toc215733097)

[9. Punkty dostępowe sieci bezprzewodowej WiFi – 7 szt. 31](#_Toc215733098)

[10. Serwer 33](#_Toc215733099)

[11. System EDR 43](#_Toc215733100)

[12. Macierz dyskowa – 2 szt. 60](#_Toc215733101)

[13. Oprogramowanie NAC - Network Access Control 62](#_Toc215733102)

# CZĘŚĆ I – Przegląd i aktualizacja dokumentacji SZBI oraz audyt końcowy bezpieczeństwa informacji Urzędzie Gminy

1. Przedmiot zamówienia obejmuje:
   1. Opracowanie i wdrożenie dokumentacji z zakresu Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z normą ISO IEC 27001 w ramach Projektu Grantowego pn. „Cyberbezpieczny Samorząd” realizowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa”.
   2. Wykonanie audytu końcowego SZBI w oparciu o Rozporządzenie Krajowych Ram Interoperacyjności, ustawę o Krajowym Systemie Cyberbezpieczeństwa, normę ISO 27001 (SZBI), wytyczne Ministerstwa Cyfryzacji dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych w ramach Projektu Grantowego pn. „Cyberbezpieczny Samorząd” realizowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa”. Audyt musi zostać zakończony szczegółowym raportem oraz wypełnieniem ankiety dojrzałości cyberbezpieczeństwa w oparciu o
2. Zakres audytu systemu bezpieczeństwa informacji każdorazowo obejmie zgodność z kryteriami zawartymi w § 19 ust. 2 ww. rozporządzenia KRI oraz zgodność z wymaganiami normy PN-EN ISO/IEC 27001:2023 dla Zamawiającego.
3. Raport z audytu KRI zostanie każdorazowo podpisany przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczony do Zamawiającego w formie elektronicznej.
4. Audyt KRI oraz aktualizacja i wdrożenie SZBI dla Zamawiającego muszą zostać przeprowadzone przez:
   1. audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. 2018 poz. 1999) lub;
   2. audytora wewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001:2023.
5. Wykonawca w trakcie realizacji zamówienia jest zobowiązany do zapoznania się z częściowo wypełnioną ankietą dojrzałości cyberbezpieczeństwa w zakresie wskazanym przez Zamawiającego oraz uwzględnić w ramach aktualizacji i wdrożenia SZBI planowany w ramach realizacji projektu zakres usprawnień SZBI.
6. Wykonawca po wykonaniu audytu końcowego jest zobowiązany do uzupełnienia ankiety dojrzałości cyberbezpieczeństwa. Ankietę dojrzałości cyberbezpieczeństwa należy wypełnić w oparciu o aktualny na dzień wypełnienia ankiety wzór ankiety opublikowany na stronie: <https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad> (załącznik nr 6 - Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego i Jednostkach Podległych).
7. Wypełnienie ankiety dojrzałości cyberbezpieczeństwa polegać będzie wypełnieniu przez Wykonawcę kolumn H, I z arkusza „Ankieta” dla Zamawiającego na podstawie zebranych przez Wykonawcę danych. Zamawiający nie dopuszcza pozostawienia pustych pól dla określonych powyżej kolumn, w przypadku jeżeli w polu opisowym nie przewiduje się zmian wówczas należy zamieścić odpowiednią informację. Ankieta dojrzałości cyberbezpieczeństwa zostanie podpisana przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczona do Zamawiającego w formie elektronicznej.
8. Wykonawca przy świadczeniu usług jest zobowiązany uwzględnić i zastosować wymagania Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) oraz akty wykonawcze wydane do niej. W przypadku jeżeli w okresie realizacji zamówienia zostanie przyjęta ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw bądź inne przepisy implementujące Dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) w polski system prawny Wykonawca ma obowiązek uwzględnić wszystkie ich wymagania przy świadczeniu usług objętych niniejszym zamówieniem zarówno w trakcie realizacji zamówienia jak i w trakcie okresu gwarancji.
9. Na wszystkie usługi Wykonawca udzieli 12-miesięcznej gwarancji polegającej na wprowadzaniu niezbędnych zmian w dokumentacji i aktualizacji dokumentacji na podstawie stwierdzonych przez Zamawiającego niezgodności dokumentacji z bieżącym stanem w okresie gwarancji.
10. Zamawiający informuje, że tam, gdzie Zamawiający opisał przedmiot zamówienia przez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, dopuszcza się rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany udowodnić, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.
11. Wykonawca, który posługuje się równoważnymi certyfikatami lub normami musi je załączyć do oferty. Przez certyfikat lub normę równoważną Zamawiający rozumie certyfikat lub normę analogiczną co do zakresu z certyfikatami lub normami wskazanymi z nazwy, który potwierdza spełnianie certyfikacji lub normy charakteryzującej się cechami właściwymi dla certyfikacji lub normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do certyfikacji.
12. **TERMINY WYKONANIA ZAMÓWIENIA**
    1. Wykonawca zobowiązuje się wykonać przedmiot zamówienia w terminie nie dłuższym niż do 30.04.2026 r., z zastrzeżeniem, że:
       1. Aktualizacja i wdrożenie SZBI zostanie przeprowadzona w terminie 90 dni od dnia zawarcia umowy, jednak nie później niż do30.03.2026 r.
       2. Audyt końcowy zostanie przeprowadzony w terminie 30 dni od zakończenia praz związanych z przeglądem i aktualizacją SZBI, jednak nie później niż później niż do 30.04.2026 r.

# CZĘŚĆ II – Przeprowadzenie szkoleń nt. bezpieczeństwa informacji dla pracowników Urzędu w ramach realizacji grantu Cyberbezpieczny Samorząd

# Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników Urzędu Gminy

1. W ramach zadania wykonawca przeprowadzi szkolenia w zakresie cyberbezpieczeństwa dla 56 pracowników samorządowych:
   1. Kadra kierownicza - 15 osób,
   2. Pracownicy – 41 osób.
   3. Administratorzy IT – 2 osób
2. Organizacja grup szkoleniowych:
   1. Kadra kierownicza – maksymalnie 6 osób w grupie warsztatowej,
   2. Kadra administracyjna – maksymalnie 15 osób w grupie warsztatowej.
3. **Ilość godzin: minimum 14 godzin.**
4. **Planowany termin szkoleń: rok 2025**
5. **Szkolenia przeprowadzone będą w laboratorium oraz sprzęcie szkoleniowym wykonawcy.**
6. **Program szkolenia:** 
   1. **System cyberbezpieczeństwa** 
      1. Podstawowe narzędzia cyberbezpieczeństwa
      2. Z czego powinien składać się skuteczny system cyberbezpieczeństwa
      3. Jak go zbudować?
   2. **Podejrzane urządzenia elektroniczne** 
      1. Przykłady zagrożeń laptopy, pendrive, smartfony
      2. Jak się przed tym chronić?
   3. **Ransomware** 
      1. Ransomware jako najczęstszy rodzaj ataków na firmy i instytucje
      2. Jak się chronić i na co zwracać uwagę aby nie paść ofiarą cyberprzestępców
   4. **Phishing jak działa i na co zwracać uwagę** 
      1. Phishing – czym jest, jak działa?
      2. Przykłady zagrożeń związanych z Phishingem
   5. **Typowe zagrożenia występujące w Internecie**
      1. Prezentacja z wykorzystanie symulatora zagrożeń internetowych
7. **Szkolenie specjalistyczne dla kadry administracyjnej (pracownicy Urządu Gminy)**
   1. Szkolenie z zakresu cyberbezpieczeństwa skierowane do pracowników jednostek organizacyjnych Gminy obejmujące co najmniej następujące obszary:
   2. wprowadzenie do cyberbezpieczeństwa:
      1. czym jest cyberbezpieczeństwo;
      2. kluczowe zagadnienia związane z cyberbezpieczeństwem;
      3. przegląd statystyk i trendów w cyberbezpieczeństwie.
   3. typy zagrożeń w cyberprzestrzeni:
      1. malware (wirusy, trojany, robaki itp.);
      2. ataki typu phishing i spear phishing;
      3. ataki DDoS;
      4. ataki ransomware;
      5. zagrożenia związane z sieciami społecznościowymi.
   4. zasady bezpieczeństwa i praktyki:
      1. zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;
      2. zasady bezpieczeństwa e-mail;
      3. bezpieczeństwo w sieciach bezprzewodowych;
      4. bezpieczne przeglądanie internetu;
      5. backup i odzyskiwanie danych.
   5. reagowanie na incydenty i planowanie awaryjne:
      1. jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem; zasady reagowania na incydenty;
      2. planowanie awaryjne i kontynuacja działalności;
      3. przegląd realnych przypadków naruszeń bezpieczeństwa
8. **Szkolenia specjalistyczne dla kadry zarządzającej urzędu z zakresu cyberbezpieczeństwa**
   1. Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla kadry zarządzającej urzędu.
   2. Szkolenie dla kadry zarządzającej z zakresu cyberbezpieczeństwa musi zawierać następującą tematykę:
      1. Wstęp do bezpieczeństwa w cyberprzestrzenii;
      2. Akty Prawne;
      3. Krajowy System Cyberbezpieczeństwa;
      4. Analiza ataków cybernetycznych;
      5. Najpopularniejsze zagrożenia;
      6. Przewodnik po metodach obrony instytucji;
      7. Cyberbezpieczeństwo osobiste;
      8. Postępowanie w pracy;
      9. ABC higieny pracy w cyberprzestrzeni;
      10. Bezpieczeństwo pracy zdalnej;
      11. Ataki socjotechniczne - czyli niewinne „wyłudzanie” danych
      12. Kampanie Phishingowe
      13. Opłacalność ataków DoS/DDoS wymierzonych w konkretną instytucję
      14. Aktualne zagrożenia wynikające z wojny w Ukrainie·
      15. Przeprowadzenie testu wiedzy;
9. **Wymagania wobec Wykonawcy:**
   1. Wykonawca oddeleguje do realizacji zadania prelegenta (prelegentów) posiadającego certyfikat Bezpieczeństwa Informacji zgodnie z normą PN-EN ISO 27001;
   2. Wykonawca przeprowadzi szkolenia w języku polskim;
   3. Wykonawca wyda każdemu uczestnikowi szkolenia certyfikat o ukończeniu szkolenia;
   4. W ramach organizacji każdego z cykli szkoleń Wykonawca zapewni materiały szkoleniowe dla wszystkich uczestników obejmujące szczegółowy zakres merytoryczny w wersji papierowej.

# Przeprowadzenie szkoleń specjalistycznych dla Informatyka Urzędu w dziedzinie technologii i cyberbezpieczeństwa

1. **Przedmiot zamówienia**
   1. Przedmiotem zamówienia jest realizacja certyfikowanego szkolenia online z zakresu systemów bezpieczeństwa klasy UTM (Unified Threat Management) dla administratorów odpowiedzialnych za bezpieczeństwo teleinformatyczne Zamawiającego.
   2. Celem szkolenia jest nabycie praktycznych umiejętności konfiguracji, utrzymania, monitorowania oraz reagowania na incydenty z wykorzystaniem platform UTM.
2. **Wymagania dotyczące wykonawcy**
   1. Wykonawca musi:
      1. Posiadać kompetencje do prowadzenia certyfikowanych szkoleń online z zakresu UTM.
      2. Zapewnić trenera z potwierdzonym doświadczeniem w pracy z rozwiązaniami UTM i bezpieczeństwem sieciowym.
      3. Wystawić imienny certyfikat ukończenia szkolenia, uznawany w branży.
3. **Forma realizacji – wyłącznie ONLINE**

Zamówienie obejmuje jedną z dwóch form dostarczenia usługi:

* 1. **Szkolenie online na żywo (live)** - Wymagania minimalne:
     1. czas trwania: co najmniej 16 godzin dydaktycznych (2 dni szkoleniowe)
     2. prowadzenie w czasie rzeczywistym
     3. praca w środowisku testowym lub symulatorze
     4. możliwość zadawania pytań i konsultacji z trenerem
     5. dostęp do materiałów szkoleniowych w formie elektronicznej
  2. **Voucher szkoleniowy** - Zamawiający dopuszcza dostarczenie vouchera umożliwiającego rejestrację na pełne szkolenie online w dowolnym dostępnym terminie, z zastrzeżeniem:
     1. **szkolenie musi być zrealizowane nie później niż do dnia 30.05.2026 r.**
     2. voucher musi zawierać:
        1. nazwę szkolenia
        2. zakres merytoryczny
        3. informacje o dostępie do platformy rejestracyjnej
        4. gwarancję dostępności terminu przed ww. datą

1. **Zakres merytoryczny szkolenia online -** Program musi obejmować co najmniej:
   1. Architektura i funkcje UTM
      1. pojęcie UTM i jego rola w cyberbezpieczeństwie
      2. moduły ochrony: firewall, IPS/IDS, AV, sandboxing, VPN, filtrowanie treści
   2. Konfiguracja UTM w środowisku praktycznym online
      1. inicjalizacja i pierwsza konfiguracja
      2. tworzenie polityk bezpieczeństwa
      3. routing i segmentacja sieci
      4. integracja z Active Directory (opcjonalnie)
   3. Moduły ochrony i inspekcji ruchu
      1. konfiguracja IPS i analiza incydentów
      2. filtrowanie URL i aplikacji
      3. ochrona antymalware i antyspam
      4. mechanizmy zapobiegania ransomware i zagrożeniom 0-day
   4. VPN w praktyce
      1. tworzenie tuneli IPsec
      2. konfiguracja SSL VPN
      3. kontrola dostępu, MFA, polityki połączeń
   5. Monitorowanie i reagowanie
      1. analiza logów i alertów
      2. dashboardy bezpieczeństwa
      3. scenariusze reakcji na incydenty
      4. integracja z SIEM/SOAR (jeśli dotyczy)
   6. Utrzymanie bezpieczeństwa
      1. kopie zapasowe i odtwarzanie konfiguracji
      2. aktualizacje i harmonogram ochrony
      3. hardening urządzeń UTM
      4. typowe błędy i dobre praktyki w JST
2. **Rezultaty szkolenia**

Po ukończeniu szkolenia uczestnik:

* 1. Otrzymuje certyfikat potwierdzający kompetencje.
  2. Zna zasady konfiguracji systemów UTM.
  3. potrafi tworzyć polityki, analizować logi i reagować na incydenty.
  4. Umie samodzielnie zarządzać VPN, IPS, filtrowaniem treści oraz modułami ochrony.
  5. Potrafi prawidłowo zabezpieczać urządzenie zgodnie z dobrymi praktykami.

1. **Termin realizacji**
   1. Szkolenie online na żywo – termin wskazany przez Zamawiającego,

lub

* 1. Realizacja szkolenia na podstawie vouchera nie później niż 30.05.2026 r.

1. **Wymagania dotyczące osoby prowadzącej szkolenie UTM**
   1. Wykonawca zapewni trenera posiadającego aktualny certyfikat potwierdzający wiedzę i kompetencje w zakresie systemów UTM (Unified Threat Management).
   2. Certyfikat musi być wydany przez producenta technologii, instytucję szkoleniową lub podmiot certyfikujący uznany na rynku IT bezpieczeństwa sieciowego.
   3. Certyfikat powinien potwierdzać umiejętności w obszarze:
   4. konfiguracji firewalli UTM,
   5. systemów IPS/IDS, VPN, filtrowania treści,
   6. zarządzania politykami bezpieczeństwa,
   7. monitorowania i reagowania na incydenty.
   8. Dokument potwierdzający kwalifikacje trenera musi zostać dostarczony Zamawiającemu przed rozpoczęciem szkolenia w formie skanu lub kopii certyfikatu.

# CZĘŚĆ III - Dostawa urządzeń i oprogramowania zwiększających odporność na cyberataki wraz z wdrożeniem

Wykonawca zobowiązany jest podać w formularzu oferty min. producenta, model/wersję oferowanego rozwiązania, typ dzięki czemu będzie można jednoznacznie określić jaki produkt został zaoferowany. Dodatkowo Zamawiający dopuszcza podanie linków dostępowych dla oferowanego n/w sprzętu dostępnych na stronach internetowych producentów.

Wszystkie dostarczone w ramach zamówienia urządzenia, komponenty oraz oprogramowanie muszą być ze sobą w pełni kompatybilne, tworzyć spójny i poprawnie funkcjonujący ekosystem oraz umożliwiać wzajemną integrację i współdziałanie zgodnie z przeznaczeniem. Niedopuszczalne jest dostarczenie rozwiązań, które uniemożliwiają pełne wdrożenie, konfigurację lub poprawne funkcjonowanie poszczególnych systemów, np. sytuacje, w których system kontroli dostępu do sieci (NAC) nie współpracuje z dostarczonymi przełącznikami sieciowymi, serwerami lub innymi komponentami. Wykonawca ponosi pełną odpowiedzialność za zapewnienie zgodności i poprawnego działania wszystkich dostarczanych elementów infrastruktury.

Wszystkie dostarczane urządzenia, komponenty oraz oprogramowanie muszą być fabrycznie nowe, wolne od wad fizycznych i prawnych, oraz pochodzić z oficjalnych kanałów dystrybucyjnych producentów, działających na terenie Rzeczypospolitej Polskiej. Niedopuszczalne jest dostarczanie sprzętu poleasingowego, regenerowanego, używanego lub pochodzącego z rynku wtórnego.

Przedmiot zamówienia obejmuje kompleksową realizację dostawy, instalacji, wdrożenia oraz pełnej konfiguracji dostarczanych urządzeń i oprogramowania. Wykonawca zobowiązany jest do dostarczenia wszystkich elementów niezbędnych do uruchomienia i prawidłowego funkcjonowania infrastruktury zgodnie z przeznaczeniem, a także do ich zainstalowania w lokalizacji wskazanej przez Zamawiającego, wykonania wszelkich wymaganych prac montażowych i integracyjnych, przeprowadzenia niezbędnych testów sprawdzających poprawność działania, a także konfiguracji systemów w sposób zapewniający ich pełną gotowość operacyjną. Ponadto Wykonawca zapewni wsparcie wdrożeniowe, szkolenie wyznaczonych pracowników oraz dostarczy pełną dokumentację powykonawczą i instruktażową.

# UTM – 1 szt.

1. **Wymagania Ogólne**
   1. System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
   2. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
   3. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.
   4. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.
   5. System wspiera protokoły IPv4 oraz IPv6 w zakresie:
      1. Firewall.
      2. Ochrony w warstwie aplikacji.
      3. Protokołów routingu dynamicznego.
2. **Redundancja, monitoring i wykrywanie awarii**
   1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
   2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
   3. Monitoring stanu realizowanych połączeń VPN.
   4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
3. **Interfejsy, Dysk, Zasilanie:**
   1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
      1. 10 portami Gigabit Ethernet RJ-45.
      2. 8 gniazdami SFP 1 Gbps.
      3. 4 gniazdami SFP+ 10 Gbps.
   2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
   3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
   4. System realizujący funkcję Firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności minimum 480 GB.
   5. System jest wyposażony w zasilanie AC.
4. **Parametry wydajnościowe:**
   1. W zakresie Firewall’a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę.
   2. Przepustowość Stateful Firewall: nie mniej niż 39 Gbps dla pakietów 512 B.
   3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps.
   4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 33 Gbps.
   5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 5 Gbps.
   6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.5 Gbps.
   7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.
5. **Funkcje Systemu Bezpieczeństwa:**

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

* 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
  2. Kontrola Aplikacji.
  3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
  4. Ochrona przed malware.
  5. Ochrona przed atakami - Intrusion Prevention System.
  6. Kontrola stron WWW.
  7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
  8. Zarządzanie pasmem (QoS, Traffic shaping).
  9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
  10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
  11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
  12. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
  13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

1. **Polityki, Firewall**
   1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
   2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
      1. Translację jeden do jeden oraz jeden do wielu.
      2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
   3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
   4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
   5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
   6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
   7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
      1. Amazon Web Services (AWS).
      2. Microsoft Azure.
      3. Cisco ACI.
      4. Google Cloud Platform (GCP).
      5. OpenStack.
      6. VMware NSX.
      7. Kubernetes.
2. **Połączenia VPN**
   1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
      1. Wsparcie dla IKE v1 oraz v2.
      2. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
      3. Obsługa protokołu Diffie-Hellman grup 19, 20.
      4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
      5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
      6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
      7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
      8. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
      9. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
      10. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
      11. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
      12. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
   2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
      1. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
   3. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
3. **Routing i obsługa łączy WAN**

W zakresie routingu rozwiązanie zapewnia obsługę:

* 1. Routingu statycznego.
  2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
  3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
  4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
  5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
  6. BFD (Bidirectional Forwarding Detection).
  7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

1. **Funkcje SD-WAN**
   1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
   2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
2. **Zarządzanie pasmem**
   1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
   2. System daje możliwość określania pasma dla poszczególnych aplikacji.
   3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
   4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
3. **Ochrona przed malware**
   1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
   2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
   3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
   4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
   5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
   6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
   7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.
   8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
   9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
   10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
4. **Ochrona przed atakami**
   1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
   2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
   3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
   4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
   5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
   6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
   7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookiesdla protokołu http.
   8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
   9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
5. **Kontrola aplikacji**
   1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
   2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
   3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
   4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
   5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
   6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
   7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
6. **Kontrola WWW**
   1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
   2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
   3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
   4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
   5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
   6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
   7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
   8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
   9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
7. **Uwierzytelnianie użytkowników w ramach sesji**
   1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
      1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
      2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
      3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
   2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
   3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
   4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
8. **Zarządzanie**
   1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
   2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
   3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
   4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
   5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
   6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
   7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
   8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
   9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
9. **Logowanie**
   1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
   2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
   3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
   4. Możliwość włączenia logowania per reguła w polityce firewall.
   5. System zapewnia możliwość logowania do serwera SYSLOG.
   6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
10. **Testy wydajnościowe oraz funkcjonalne**
    1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.
11. **Serwisy i licencje**
    1. Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres do 30.06.2026 r.
12. **Rozszerzone wsparcie serwisowe AHB/SOS**
    1. System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres do 30.06.2026 r.
    2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7 Wymagania powinny być potwierdzone dokumentami:
    3. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:
       1. Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
       2. Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
       3. Doradztwo w zakresie konfiguracji.
       4. Zdalne wsparcie techniczne.
       5. Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
       6. Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
       7. Przygotowanie urządzenia do zdalnej konfiguracji.
       8. Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
    4. Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.
       1. Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
       2. Certyfikat ISO 9001 podmiotu serwisującego.
13. **Opisy do wymagań ogólnych**
    1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
    2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

# Przełączniki sieciowe Typ 1 – 2 szt.

1. **Przełącznik sieciowy**
   1. W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.
2. **Parametry fizyczne platformy**
   1. Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
   2. Zasilanie AC 230V.
   3. Maksymalny pobór mocy: 30 W.
   4. Minimalny zakres temperatury pracy: 0-40ᵒC.
3. **Interfejsy sieciowe - wymagania minimalne**
   1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
      1. 24 porty GE RJ-45.
      2. 4 porty 10 GE SFP+.
4. **Zarządzanie**
   1. Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
   2. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
   3. Wsparcie dla SNMP w wersjach 1-3
   4. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
   5. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
   6. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
   7. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
   8. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
   9. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
   10. Automatycznie wykonywane rewizje konfiguracji.
5. **Parametry wydajnościowe**
   1. Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps.
   2. Tablica adresów MAC o pojemności co najmniej 32k wpisów.
   3. Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
6. **Wymagane funkcje**
   1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
   2. Obsługa Jumbo Frames.
   3. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
   4. Agregacja portów zgodna ze standardem 802.3ad.
   5. Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
   6. Obsługa routingu statycznego.
   7. Port-mirroring.
   8. Uwierzytelnianie 802.1x na poziomie portu.
   9. Uwierzytelnianie 802.1x w oparciu o adres MAC.
   10. W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
   11. W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
   12. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
   13. Obsługa protokołu sFlow.
7. **Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC**
   1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
      1. Centralne zarządzanie konfiguracją urządzenia
      2. Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
      3. Centralne zarządzanie sieciami VLAN.
      4. Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
      5. Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
      6. Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
      7. Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
      8. Automatyczna detekcja i rekomendacje konfiguracji.
      9. Przesyłanie logów na zewnętrzny serwer syslog.
      10. Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
      11. Obsługa białych i czarnych list adresów MAC.
      12. Wykrywanie aplikacji komunikujących się w sieci.
   2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
   3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
8. **Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa**
   1. System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
   2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
9. **Gwarancja oraz wsparcie**
   1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

# Przełączniki sieciowe Typ 2 – 6 szt.

1. **Przełącznik sieciowy**
   1. W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.
2. **Parametry fizyczne platformy**
   1. Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
   2. Zasilanie AC 230V.
   3. Maksymalny pobór mocy: 10 W.
   4. Minimalny zakres temperatury pracy: 0-40ᵒC.
3. **Interfejsy sieciowe - wymagania minimalne**
   1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
      1. 8 porty GE RJ-45.
      2. 2 porty GE, SFP.
4. **Zarządzanie**
   1. Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
   2. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
   3. Wsparcie dla SNMP w wersjach 1-3
   4. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
   5. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
   6. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
   7. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
   8. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
   9. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
   10. Automatycznie wykonywane rewizje konfiguracji.
5. **Parametry wydajnościowe**
   1. Przepustowość urządzenia - min. 20 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 30 Mpps.
   2. Tablica adresów MAC o pojemności co najmniej 8 k wpisów.
   3. Opóźnienie wprowadzane przez przełącznik - poniżej 5 mikrosekund.
6. **Wymagane funkcje**
   1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
   2. Obsługa Jumbo Frames.
   3. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
   4. Agregacja portów zgodna ze standardem 802.3ad.
   5. Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
   6. Obsługa routingu statycznego.
   7. Port-mirroring.
   8. Uwierzytelnianie 802.1x na poziomie portu.
   9. Uwierzytelnianie 802.1x w oparciu o adres MAC.
   10. W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
   11. W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
   12. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
7. **Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC**
   1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
      1. Centralne zarządzanie konfiguracją urządzenia
      2. Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
      3. Centralne zarządzanie sieciami VLAN.
      4. Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
      5. Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
      6. Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
      7. Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
      8. Automatyczna detekcja i rekomendacje konfiguracji.
      9. Przesyłanie logów na zewnętrzny serwer syslog.
      10. Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
      11. Obsługa białych i czarnych list adresów MAC.
      12. Wykrywanie aplikacji komunikujących się w sieci.
   2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
   3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
8. **Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa**
   1. System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
   2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
9. **Gwarancja oraz wsparcie**
   1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

# Przełącznik sieciowy typ 3 – 1 szt.

1. **Przełącznik sieciowy**
   1. W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.
2. **Parametry fizyczne platformy**
   1. Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
   2. Zasilanie AC 230V.
   3. Budżet mocy dla portów PoE min.: 370 W.
   4. Maksymalny pobór mocy bez budżetu dla PoE: 85 W.
   5. Minimalny zakres temperatury pracy: 0-40ᵒC.
3. **Interfejsy sieciowe - wymagania minimalne**
   1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
      1. 24 porty GE RJ-45.

W tym porty PoE w ilości co najmniej: 24, zgodne ze standardem: 802.3af oraz 802.3at.

* + 1. 4 porty 10 GE SFP+.

1. **Zarządzanie**
   1. Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
   2. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
   3. Wsparcie dla SNMP w wersjach 1-3
   4. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
   5. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
   6. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
   7. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
   8. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
   9. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
   10. Automatycznie wykonywane rewizje konfiguracji.
2. **Parametry wydajnościowe**
   1. Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps.
   2. Tablica adresów MAC o pojemności co najmniej 32k wpisów.
   3. Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
3. **Wymagane funkcje**
   1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
   2. Obsługa Jumbo Frames.
   3. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
   4. Agregacja portów zgodna ze standardem 802.3ad.
   5. Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
   6. Obsługa routingu statycznego.
   7. Port-mirroring.
   8. Uwierzytelnianie 802.1x na poziomie portu.
   9. Uwierzytelnianie 802.1x w oparciu o adres MAC.
   10. W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
   11. W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
   12. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
   13. Obsługa protokołu sFlow.
4. **Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC**
   1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
      1. Centralne zarządzanie konfiguracją urządzenia
      2. Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
      3. Centralne zarządzanie sieciami VLAN.
      4. Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
      5. Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
      6. Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
      7. Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
      8. Automatyczna detekcja i rekomendacje konfiguracji.
      9. Przesyłanie logów na zewnętrzny serwer syslog.
      10. Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
      11. Obsługa białych i czarnych list adresów MAC.
      12. Wykrywanie aplikacji komunikujących się w sieci.
   2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
   3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
5. **Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa**
   1. System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
   2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
6. **Gwarancja oraz wsparcie**
   1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

# Przełączniki sieciowe typ 4 – 2 szt.

1. **Przełącznik sieciowy**
   1. W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.
2. **Parametry fizyczne platformy**
   1. Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
   2. Zasilanie AC 230V.
   3. Maksymalny pobór mocy: 60 W.
   4. Minimalny zakres temperatury pracy: 0-40ᵒC.
3. **Interfejsy sieciowe - wymagania minimalne**
   1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
      1. 48 porty GE RJ-45.
      2. 4 porty 10 GE SFP+.
4. **Zarządzanie**
   1. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
   2. Wsparcie dla SNMP w wersjach 1-3
   3. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
   4. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
   5. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
   6. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
   7. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
   8. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
   9. Automatycznie wykonywane rewizje konfiguracji.
5. **Parametry wydajnościowe**
   1. Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.
   2. Tablica adresów MAC o pojemności co najmniej 32k wpisów.
   3. Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
6. **Wymagane funkcje**
   1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
   2. Obsługa Jumbo Frames.
   3. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
   4. Agregacja portów zgodna ze standardem 802.3ad.
   5. Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
   6. Obsługa routingu statycznego.
   7. Port-mirroring.
   8. Uwierzytelnianie 802.1x na poziomie portu.
   9. Uwierzytelnianie 802.1x w oparciu o adres MAC.
   10. W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
   11. W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
   12. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
   13. Obsługa protokołu sFlow.
7. **Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC**
   1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
      1. Centralne zarządzanie konfiguracją urządzenia
      2. Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
      3. Centralne zarządzanie sieciami VLAN.
      4. Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
      5. Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
      6. Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
      7. Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
      8. Automatyczna detekcja i rekomendacje konfiguracji.
      9. Przesyłanie logów na zewnętrzny serwer syslog.
      10. Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
      11. Obsługa białych i czarnych list adresów MAC.
      12. Wykrywanie aplikacji komunikujących się w sieci.
   2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
   3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
8. **Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa**
   1. System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
   2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
9. **Gwarancja oraz wsparcie**
   1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

# Agregat

1. Przedmiotem zamówienia jest dostawa nowego agregatu prądotwórczego zabudowanego w obudowie dźwiękochłonnej dla rezerwowego zasilania.
2. Przedmiot zamówienia obejmuje dostawę i pierwsze uruchomienie agregatu prądotwórczego wraz z podzespołami.
3. **Zakres robót**

Zakres robót obejmuje:

* 1. napełnienie płynami eksploatacyjnymi oraz zapewnienie paliwa ze zbiornika zewnętrznego w ilości niezbędnej do przeprowadzenia testów według procedury dostawcy (z wyłączeniem wielogodzinnych prób pod obciążeniem),
  2. dostawę i pierwsze uruchomienie agregatu prądotwórczego zabudowanego z automatycznym i manualnym rozruchem o mocy znamionowej min. 36,0 kW,
  3. przeprowadzenie szkolenia pracowników w zakresie obsługi agregatu wraz z podzespołami.

1. **Montaż**
   1. Pierwsze uruchomienie agregatu nastąpi w dedykowanym i przygotowanym przez Zamawiającego punkcie przyłącza Urzędu Miasta i Gminy Małkinia Górna.
2. **Warunki gwarancji i serwisu**
   1. Producent udzieli gwarancji na bezawaryjną pracę zespołu prądotwórczego wraz z ewentualnym wyposażeniem dodatkowym na okres 24 miesięcy lub 1000 mth, licząc od daty sprzedaży bezpośredniemu użytkownikowi (w zależności, co nastąpi wcześniej).
   2. Wykonawca uwzględni w cenie oferty niezbędne przeglądy konserwacyjne.
3. **Dokumentacja** 
   1. Wraz z dostawą agregatu Wykonawca zobowiązany jest przekazać następujące dokumenty:
      1. instrukcja obsługi agregatu i sterownika,
      2. Dokumentację potwierdzającą spełnianie następujących Dyrektyw i Norm:
         1. 2006/42/WE Dyrektywa Maszynowa
         2. Kompatybilność elektromagnetyczna 2014/30/UE.
         3. 2014/35/UE sprzętu elektrycznego przewidzianego do stosowania w określonych granicach napięcia
         4. PN-EN ISO 8528-13:2016-07
         5. PN- EN ISO 3744:2011
         6. ISO 8528-1:2005
         7. 2000/14/WE, 2005/88/WE – Dyrektywa Hałasowa
         8. Klasa wykonania minimum G2.
         9. Wymagane jest aby agregat pochodził z seryjnej i bieżącej produkcji.
4. **Agregat prądotwórczy**
   1. Wymagana moc znamionowa agregatu – 45 kVA (36 kW).
   2. Wymagana moc awaryjna agregatu nie mniej niż – 50 kVA (40 kW).
   3. Napięcie – 400/230 V.
   4. Częstotliwość – 50Hz.
   5. Powinien być wyprodukowany w Polsce lub na terenie UE i posiadać oznaczenie CE.
   6. Dostarczone urządzenie powinno być w całości spreparowane przez jednego producenta posiadającego:
      1. wdrożony system ISO 9001:2015,
      2. wdrożony system AQAP 2110:2016
      3. deklarację CE dla agragatu
   7. Jakiekolwiek modyfikacje urządzenia ingerujące w jego konstrukcję nie są dopuszczane.
5. **Obudowa**
   1. Obudowa dźwiękochłonna, wyciszona, niepalną pianką wygłuszającą, z drzwiami dostępowymi na dłuższych bokach.
   2. Stalowy tłumik dźwięków -35db(A) – zabudowany wewnątrz agregatu
   3. Wylot spalin i gorącego powietrza poprzez górną połać obudowy.
   4. Podejście kablowe, umożliwiające wprowadzenie okablowania bez wychodzenia kablami poza obrys agregatu.
   5. Wytrzymała konstrukcja z możliwością transportu wózkiem widłowym, dźwigiem, HDS – na pasach, widłach lub łańcuchach.
   6. Rama dodatkowo izolowana od podłoża za pomocą stóp przykręcanych do ramy, z możliwością regulacji wysokości (poziomowania).
   7. Zewnętrzny przycisk zatrzymania awaryjnego.
   8. Wymiary nieprzekraczające (dł. x szer. x wys.) – 2300 x 1500 x 1540 [mm]
   9. Zamontowane amortyzatory drgań silnika i prądnicy.
   10. Gwarantowany poziom mocy akustycznej – nie więcej niż 97 dB (A)
6. **Zbiornik paliwa**
   1. Zbiornik paliwa, w ramie agregatu, pozwalający na ciągłą pracę agregatu:
      1. przy 75% obciążeniu, co najmniej 8,9 h,
      2. przy 100% obciążeniu, co najmniej 6,9 h.
   2. Wlew paliwa zamykany kluczykiem, wewnątrz obudowy.
   3. Wymagany korek spustowy zbiornika oraz co najmniej jeden niezależny, zaślepiony otwór w zbiorniku, umożliwiający montaż i podłączenie dodatkowej instalacji paliwowej, lub przeniesienie wlewu paliwa na drugą stronę zbiornika.
7. **Silnik**
   1. Typ Silnika - Diesel
   2. Liczba i układ cylindrów – 4 L.
   3. Wymagany typ wtrysku – bezpośredni.
   4. Elektroniczna regulacja obrotów.
   5. Emisja spalin - non emission
   6. Podgrzewanie bloku – grzałka silnika kontrolowana przez sterownik agregatu.
   7. Spalanie przy 75% obciążenia nie więcej niż – 11,4 l/h.
   8. Spalanie przy 100% obciążenia nie więcej niż – 14,6 l/h.
   9. Wlew paliwa - korek zamykany kluczykiem, wewnątrz obudowy.
   10. Filtr powietrza suchy.
   11. Silnik chłodzony glikolem.
   12. Prędkość obrotowa – 1500 r.p.m.
   13. Układ elektryczny 12V lub 24V.
   14. Akumulator 12V (lub 2x12V)
   15. Automatyczna ładowarka buforowa akumulatora/ów 12Vlub 24V/5A w czasie czuwania.
   16. Osłona elementów gorących oraz ruchomych.
8. **Prądnica**
   1. Prądnica wyposażona w automatyczną regulację napięcia
   2. Szczelność Obudowy (wg IEC-34-5) - IP23.
   3. Złącze – elastyczny dysk.
   4. Klasa izolacji – H.
   5. Zaimplementowane rozwiązanie minimalizujące indukowanie się nadmiernych prądów w obwodzie neutralnym.
   6. Wytrzymałość zwarciowa prądnicy >300% obciążenia znamionowego.
9. **Sterownik**
   1. Graficzny wyświetlacz LCD 128x64
   2. Komunikaty w języku polskim
   3. Monitoring parametrów sieci i agregatu (napięć, prądów, mocy, częstotliwości, cos ɸ, napięcia ładowania akumulatora, ilość paliwa w zbiorniku, czasu pracy agregatu, parametrów silnika).
   4. Dziennik na min. 400 zdarzeń,
   5. Panel sterownika wyposażony w tabliczkę z diodami sygnalizacyjnymi dla łatwej obsługi i szybkiej identyfikacji stanów pracy urządzenia. Wymagana jest identyfikacja alarmów dotyczących działania baterii, pracy alternatora, poziomu paliwa, ciśnienia oleju oraz możliwość zdefiniowania co najmniej dwóch dodatkowych alarmów we własnym zakresie.
   6. Sterownik musi posiadać w tylnej ścianie wolne sloty do podłączenia dodatkowych modułów sygnalizacyjnych np. GSM, ETHERNET, styków/wyjść przekaźnikowych dla sygnałów bezpotencjałowych (do zdefiniowania przez użytkownika).
   7. Min. 6 konfigurowalnych wyjść cyfrowych
   8. Min. 3 konfigurowalne wejścia analogowe
10. **Funkcje bezpieczeństwa**
    1. Osłona elementów gorących oraz ruchomych.
    2. Ochrona przed nadmierną mocą
    3. Odwrotna ochrona zasilania
    4. Zabezpieczenie przed przeciążeniem IDMT
    5. Zrzut obciążenia, obciążenie zastępcze
    6. Zarządzanie wieloma obciążeniami
    7. Zabezpieczenie od asymetrii prądu
    8. Ochrona przed asymetrią napięcia
11. **Pomiary**
    1. Napięcia sieci i agregatu PN / PP
    2. Częstotliwość sieci i agregatu
    3. Prądy fazowe sieci i agregatu
    4. Prądy neutralne sieci i agregatu
    5. Sieć i agregat, faza i suma, kW, kVA, kVAr, pf
    6. Prędkość silnika
    7. Napięcie baterii
    8. Temperatura silnika
    9. Ciśnienie oleju
    10. Zużycie paliwa (dla silników wyposażonych w ECU)
12. Dla pełnego wsparcia wymagane jest:
    1. aby u producenta urządzenia wdrożono normę PN-EN ISO 9001:2015 lub równoważną, w zakresie co najmniej produkcji lub projektowania lub rozwoju - urządzeń lub systemów lub rozwiązań podtrzymania zasilania (producent posiada certyfikat ISO 9001:2015 lub równoważny).
    2. aby dostawca całości urządzeń i usług w ramach zadania Cyberbezpieczny Samorząd posiadał umowę o współpracy z producentem agregatu w zakresie dostawy, uruchomienia i serwisowania dostarczonych maszyn i urządzeń dodatkowych.
    3. aby producent agregatu posiadał w Polsce własny oddział, serwis oraz magazyn części zamiennych i materiałów eksploatacyjnych.
13. **Próby fabryczne**
    1. Przed dostarczeniem agregatu na obiekt należy wykonać próby FAT u producenta - na życzenie Zamawiającego w obecności komisji oddelegowanej przez Zamawiającego – i załączyć ich wyniki do protokołu odbioru.

## 

# Zasilacz UPS stanowiskowy – typ 1 – 54 szt.

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Moc pozorna | 1. min. 550VA |
| Moc rzeczywista | 1. min. 330W |
| Technologia | 1. VI (line interactive) |
| Typ obudowy | 1. wolnostojąca |
| **Praca sieciowa** | |
| Napięcie wejściowe | 1. 162 ÷ 290 V AC ± 7 % |
| Częstotliwość napięcia wejściowego | 1. 40 ÷ 70 Hz ± 1 Hz |
| Zakres napięcia wyjściowego | 1. 230 V AC ± 10 % |
| Kształt napięcia wyjściowego (przy pracy rezerowej/sieiowej) | 1. Schodkowa aproksymacja sinusoidy / Tak jak na wejściu |
| Progi przełączania sieć – UPS | 1. 162 ÷ 290 V AC ± 7 % |
| Czas przełączania sieć – UPS | 1. <6ms |
| **Praca bateryjna** | |
| Napięcie wyjściowe | 1. ~230V ± 10% |
| Częstotliwość napięcia wyjściowego | 1. 50 / 60 Hz ± 1% |
| Kształt napięcia wyjściowego na pracy bateryjnej | 1. Schodkowa aproksymacja sinusoidy |
| Progi przełączania UPS – sieć | 1. ~172 ÷ 280 V ± 7 V |
| Przeciążalność | 1. > 110% - 1 min (wyłączenie UPS – praca sieciowa i bateryjna) |
| Zabezpieczenie wyjściowe przeciwzwarciowe | 1. elektroniczne |
| Zabezpieczenie wyjściowe przeciążeniowe | 1. elektroniczne |
| Czas podtrzymania (P 0,8max/P 0,5max) | 1. minimum 2/6 min |
| akumulatory wewnętrzne | 1. minimum 12V5Ah; szczelne, bezobsługowe VRLA |
| **Pozostałe** | |
| Wejście zasilania | 1. Przewód zakończony wtyczką z uziemieniem 16A (PN-E-93201:1997) + uni schucko |
| Ilość i typ gniazd wyjściowych | 1. minimum 4x IEC 320 C13 (10 A) |
| Sygnalizacja | 1. Akustyczno-optyczna 2. Dioda syngnalizująca minimum pracę sieciową, bateryjną, niski poziom baterii, przeciążenie, awarię 3. Sygnalizacja akustyczna informująca o minimum pracy bateryjnej, niskim poziomie baterii, przeciążeniu, awarii |
| Zimny Start | 1. tak |
| Interfejs komunikacyjny | 1. USB HID (kabel w komplecie) |
| Automatyczna regulacja napięcia AVR | 1. wymagana |
| Waga UPS | 1. do 4kg |
| Wymiary | 1. nie większe niż: wysokość 160mm; szerokość 85mm; głębokość 255mm |
| Gwarancja | 1. min 24 miesiące na elektronikę i 12 miesięcy na akumulatory; |
| Serwis | 1. autoryzowany serwis producenta zlokalizowany w Polsce. 2. serwis realizowany w systemie door-to-door |
| Oprogramowanie | 1. jedno uniwersalne oprogramowanie do zarządzania oferowanymi urządzeniami UPS 2. oprogramamowanie w języku polskim do zarządzania i monitorowania pracy UPS . 3. wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. 4. możliwość edycji nazw urządzeń na liście monitorowanych UPSów 5. wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer |
| Certyfikaty producenta (załączyć do oferty) | 1. ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania; 2. deklaracja CE producenta sprzętu |
| Oświadczenia / dokumenty | 1. oświadczenie producenta o spełnieniu minimlanych wymaganych parametrów specyfikacji 2. oświadczenie producenta o możliwosci udostepnienia przed dostawą 1 sztuki wyrobu na testy w ciągu 3 dni roboczych od wezwania przez zamawiającego 3. Oświadczenie producenta o posiadaniu licencji oraz pełnych praw do oprogramowania do monitorowania pracy UPS 4. karta katalogowa oferowanego sprzętu |

# Zasilacz UPS - Typ 2 – 2 szt.

1. **Typ urządzenia:**  
   Zasilacz awaryjny typu line-interactive, montowany w szafie rack 19", wysokość maksymalnie 2U.
2. **Moc wyjściowa:**
   1. Moc pozorna: nie mniej niż 2200 VA
   2. Moc czynna: nie mniej niż 1980 W
3. **Forma napięcia wyjściowego:**  
   Czysta fala sinusoidalna.
4. **Napięcie wejściowe i wyjściowe:**
   1. Napięcie nominalne: 230 V AC
   2. Zakres napięcia wejściowego: min. 160–286 V
   3. Zakres częstotliwości: 50/60 Hz ±3 Hz
5. **Czas podtrzymania:**
   1. Dla obciążenia 100%: minimum 4 min
   2. Dla obciążenia 50%: minimum 13 min
6. **Złącza wyjściowe:**
   1. Min. 9 gniazd wyjściowych zasilających typu IEC C13/C19 (lub równoważne), umożliwiających podłączenie urządzeń IT.
7. **Zarządzanie i monitorowanie:**
   1. Interfejs komunikacyjny: port USB i/lub port szeregowy
   2. Możliwość zarządzania zdalnego przez sieć LAN (integracja z chmurą lub systemem zarządzania zasilaniem)
   3. Wbudowany wyświetlacz LCD z informacjami o stanie urządzenia, parametrach pracy oraz alertami
8. **Baterie:**
   1. Wymienne przez użytkownika
   2. Typ: bezobsługowe, szczelne (np. AGM)
   3. Możliwość podłączenia zewnętrznych modułów bateryjnych (opcjonalnie)
9. **Ochrona:**
   1. Zabezpieczenie przed przeciążeniem, przepięciem, zwarciem
   2. Filtracja zakłóceń EMI/RFI
   3. Automatyczna regulacja napięcia (AVR)
10. **Pozostałe wymagania:**
    1. Montaż w szafie rack 19"
    2. W zestawie zestaw montażowy
    3. Waga: nie więcej niż 30 kg
    4. Gwarancja: minimum 36 miesięcy (z wymianą urządzenia na nowy lub naprawą na miejscu instalacji)

# Punkty dostępowe sieci bezprzewodowej WiFi – 7 szt.

**Access Point**

1. Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.
2. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
   1. Temperatura 0–50°C,
   2. Wilgotność 5–90%.
3. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie

przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona

w złącze typu Kensington.

1. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych

poniżej pasmach i obsługiwać co najmniej następujące standardy:

* 1. 2.4 GHz 802.11b/g/n,
  2. 5 GHz 802.11a/n/ac/ax,
  3. 6 GHz 802.11ax/be

1. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.
2. Urządzenie musi być wyposażone w moduł BLE.
3. Urządzenie musi być wyposażone w co najmniej jeden interfejs Ethernet (RJ45) wspierający

co najmniej szybkości 1G/2.5G/5.0G.

1. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny

zasilacz. Maksymalne zużycie energii nie może przekraczać 17W przy wykorzystaniu

wszystkich funkcji urządzenia.

1. 8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
   1. Tunnel,
   2. Bridge,
   3. Mesh.
2. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
3. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist &amp; whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST).
4. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
   1. MIMO – 2x2,
   2. Wymagana maksymalna przepustowość dla poszczególnych modułów radiowych:
      1. 688 Mbps;
      2. 2882 Mbps;
      3. 5765 Mbps;
   3. Wymagana moc nadawania:
      1. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
      2. min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
      3. min. 22 dBm dla pasma 6GHz z możliwością zmiany co 1dBm
   4. Wsparcie dla kanałów 20/40/80/160/320MHz,
   5. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5dBi dla pasma 6GHz.
   6. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy.
   7. Każdy z modułów radiowych musi posiadać możliwość pracy jako dedykowany skaner.
5. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512
6. Funkcje dodatkowe:
   1. OFDMA UL i DL
   2. Spatial Reuse (BSS Coloring)
   3. UL-MU-MIMO
   4. DL-MU-MIMO
   5. Enhanced Target Wake Time (TWT)
   6. Wbudowany analizator widma
   7. Wbudowane mechanizmy WIPS/WIDS
7. Gwarancja oraz wsparcie
   1. Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

# Serwer

| **Parametr** | **Charakterystyka (wymagania minimalne) - Serwer** |
| --- | --- |
| **Obudowa** | 1. Obudowa Rack o wysokości max 1U 2. 8 wnęk na dyski 2.5” 3. Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serweraw tym adres IP karty zarządzającej 4. 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** | 1. Płyta główna z możliwością zainstalowania do dwóch procesorów. 2. Obsługa procesorów 32 rdzeniowych. 3. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. 4. Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. 5. Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| **Chipset** | 1. Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| **Procesor** | 1. Zainstalowany procesor, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 169 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji jedno lub dwuprocesorowej. |
| **RAM** | 1. 128GB DDR5 RDIMM 5600MT/s, |
| **Kontroler RAID** | 1. Sprzętowy kontroler dyskowy, posiadający    1. Min. 8GB nieulotnej pamięci cache,    2. Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.    3. Wsparcie dla dysków samoszyfrujących |
| **Dyski twarde** | 1. Zainstalowane    1. 5x dysk SAS 12Gb o pojemności min. 600GB Hot-Plug. 2. Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB z możliwością konfiguracji RAID 1. |
| **Gniazda PCI** | 1. Dwa sloty PCIe LP |
| **Interfejsy sieciowe/FC/SAS** | 1. Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |
| **Wbudowane porty** | 1. 4 porty USB w tym min:    1. 1 port USB 3.0 z tyłu obudowy,    2. 1 port micro USB z przodu obudowy 2. 2 port VGA z czego jeden z przodu obudowy 3. Możliwość rozbudowy o port RS232 |
| **Video** | 1. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| **Zasilacze** | 1. Redundantne, Hot-Plug min. 700W klasy Titanium |
| **Elementy montażowe** | 1. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |
| **Bezpieczeństwo** | 1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. 2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. 3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła 4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. 5. Moduł TPM 2.0 6. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera 7. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem 8. Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| **System operacyjny oraz licencje dostępowe** | 1. Windows Server 2022 Standard – licencja dobrana tak, aby przy oferowanych procesorach umożliwić uruchomienie 2 maszyn wirtualnych. 2. Microsoft Windows Server 2022 Standard lub równoważny spełniający min. poniższe wymagania: 3. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. 4. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. 5. 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. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 7. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 8. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 9. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. 10. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading; 11. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 12. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 13. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. 14. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 15. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji. 18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 20. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). 21. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 22. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 23. Możliwość migracji konfiguracji systemu Microsoft Windows Serwer 2021/2016. 24. Zamawiający wymaga zapewnienia minimum 65 jednoczesnych Call dostępowych (licencji dostępowych) przypisanych per użytkownik, umożliwiających równoczesne korzystanie z systemu |
| **Karta Zarządzania** – w formularzu oferty należy podać pełną nazwę oferowanej karty | 1. Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. 2. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Oprogramowanie do zarządzania** – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | 1. Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego, automatycznie tworzące zgłoszenia serwisowe w przypadku awarii. 2. Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera. 3. Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów. 4. Konfiguracja i zaoferowany poziom wsparcia powinien po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia powinien się kontaktować z klientem w celu rozwiązania problemu. 5. Oprogramowanie musi współpracować z kartą do zarządzania w urządzeniu, która będzie działać niezależnie od zainstalowanego systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit. Karta musi umożliwiać podmontowanie zdalnych wirtualnych napędów, oraz wirtualną konsolę z dostępem do myszy, klawiatury. 6. Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :    1. Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień.    2. Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów.    3. Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta.    4. upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,    5. możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :       1. o poprawkach i usprawnieniach dotyczących aktualizacji       2. dacie wydania ostatniej aktualizacji       3. priorytecie aktualizacji       4. zgodność z systemami operacyjnymi       5. jakiego komponentu sprzętu dotyczy aktualizacja       6. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu 63.5.1. do punktu 63.5.5.    6. wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne    7. możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.    8. -rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty ( dd-mm-rrrr )    9. sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą ( dd-mm-rrrr ) i wersją ( rewizja wydania )    10. dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml        1. raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml od razu spakowany z rozszerzeniem \*.zip. Raport musi zawierać z dokładną datą ( dd-mm-rrrr ) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. |
| **Oprogramowanie do monitorowania** – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | 1. Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: 2. **Monitoring:**    1. ilość podłączonych oraz rozłączonych systemów    2. stan podłączonych urządzeń    3. informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów    4. Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia    5. informacje o statusie gwarancji dla poszczególnych urządzeń    6. informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń    7. informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.    8. Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych    9. 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.    10. Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.    11. Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.    12. Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.    13. Monitoring parametrów serwerów z informacją o minimum:        1. Obciążeniu procesora        2. Zużyciu pamięci RAM        3. Temperaturze procesorów        4. Temperaturze powietrza wlotowego        5. Zużyciu prądu        6. Zmianach w fizycznej konfiguracji serwera        7. Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.    14. Monitoring parametrów pamięci masowych z informacją o minimum:        1. Opóźnieniach        2. IOPS        3. Przepustowości        4. Utylizacji kontrolerów        5. Pojemność całkowita i dostępna        6. Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.        7. Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.        8. Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata        9. Informacje o poziomie redukcji danych        10. Informacje o statusie replikacji oraz snapshotów    15. Monitoring parametrów przełączników sieciowych z informacją o minimum:        1. Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny        2. Stanie komponentów: zasilacze, wentylatory        3. Podłączonych hostach        4. Ilości i statusu portów        5. Utylizacji procesora        6. Utylizacji poszczególnych portów        7. Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. 3. **Aktualizacja firmware**    1. możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania    2. możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania    3. możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania    4. możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania    5. możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania 4. **Raporty**    1. Możliwość generowania raportów dla serwerów zawierających informację o:       1. Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej       2. Średnim obciążeniu: procesorów, pamięci RAM, IO,    2. Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:       1. 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       2. Generowanie raportów do plików CSV i PDF 5. **Cyberbezpieczeństwo**    1. 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.    2. Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.    3. Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.    4. Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. 6. Wspierane urządzenia    1. Urządzenie Producenta dostarczane w ramach postępowania    2. Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) 7. Wirtualny asystent    1. 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; 8. Możliwość rozszerzenia funkcjonalności    1. Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. 9. **Inne**    1. Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android 10. **Certyfikaty**     1. Oferowana platforma musi być zaprojektowana zgodnie ze standardami:        1. ISO 27001        2. NIST Security and Privacy Controls for Federal Information Systems and Organization     2. CSA Cloud Control Matrix |
| **Certyfikaty** | 1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 2. Serwer musi posiadać deklaracja CE. 3. 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](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** 4. 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** | 1. Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. 2. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Wsparcie techniczne i oprogramowanie** – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | 1. Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego, 2. automatycznie tworzące zgłoszenia serwisowe w przypadku awarii. 3. Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera. 4. Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów. 5. Konfiguracja i zaoferowany poziom wsparcia powinien po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia powinien się kontaktować z klientem w celu rozwiązania problemu. 6. Oprogramowanie musi współpracować z kartą do zarządzania w urządzeniu, która będzie działać niezależnie od zainstalowanego systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit. Karta musi umożliwiać podmontowanie zdalnych wirtualnych napędów, oraz wirtualną konsolę z dostępem do myszy, klawiatury. 7. Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :    1. Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień.    2. Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów.    3. Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta.    4. upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,    5. możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :       1. o poprawkach i usprawnieniach dotyczących aktualizacji       2. dacie wydania ostatniej aktualizacji       3. priorytecie aktualizacji       4. zgodność z systemami operacyjnymi       5. jakiego komponentu sprzętu dotyczy aktualizacja       6. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu 57.5.1 do punktu 57.5.5    6. wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne    7. możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.    8. - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty ( dd-mm-rrrr )    9. sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą ( dd-mm-rrrr ) i wersją ( rewizja wydania )    10. dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml    11. raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml od razu spakowany z rozszerzeniem \*.zip. Raport musi zawierać z dokładną datą ( dd-mm-rrrr ) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. |
| **Warunki gwarancji** | 1. Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. 2. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. 3. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. 4. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 5. 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 zakończenia diagnostyki. 6. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 7. 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. 8. 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. 9. Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:    1. Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.    2. 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.    3. Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.    4. 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.    5. 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 Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. 10. **Wymagane dołączenie do oferty** oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. 11. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – **dokumenty potwierdzające należy załączyć do oferty.** |

# System EDR

| **Parametr** | **Wymagania minimalne – system EDR** |
| --- | --- |
| **LICENCJA** | W ramach postępowania Wykonawca jest zobowiązany dostarczyć:   1. Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć licencje czasową na 12 miesięcy. 2. Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru, min. 2-letniągwarancję producenta Oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania). 3. Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji w okresie gwarancji. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do serwisu producenta. 4. Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej. 5. Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych. 6. Ilość licencji dla komputerów: 100 7. Ilość licencji dla serwerów: 6 |
| **Ochrona punktów końcowych urządzeń komputerowych** – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | 1. Ochrona antywirusowa niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową. 2. Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta. 3. Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EPP i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej. 4. Rozwiązanie dla ochrony antywirusowej stacji roboczych wspiera następujące systemy operacyjne:    1. Microsoft Windows 10    2. Microsoft Windows 11    3. MacOS version 14 "Sonoma"    4. MacOS version 13 "Ventura"    5. MacOS version 12 "Monterey" 5. Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:    1. Microsoft Internet Explorer    2. Microsoft Edge    3. Mozilla Firefox    4. Google Chrome    5. Safari 6. Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika. 7. Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej. 8. Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej 9. Oprogramowanie instalowane na stacjach końcowych, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku. 10. Agent instalowany na stacjach końcowych posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory. 11. Agent instalowany na stacjach końcowych posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania. 12. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych. 13. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń. 14. Agent instalowany na stacjach końcowych monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:     1. dostęp do pliku;     2. tworzenie nowego procesu;     3. nawiązane połączenia sieciowe;     4. wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;     5. zawartość skryptów uruchamianych na monitorowanej stacji. 15. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej. 16. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych. 17. Komunikacja agentów instalowanych na stacjach roboczych, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS. 18. Komunikacja agentów instalowanych na stacjach roboczych, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy). 19. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet. 20. Dane zbierane przez agentów na stacjach końcowych są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej. 21. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych. 22. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego. 23. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych w środowisku informatycznym. 24. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami. 25. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii. 26. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym. 27. Każda detekcja zawiera co najmniej następujące informacje:     1. Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.     2. Data i czas wystąpienia podejrzanych zdarzeń.     3. Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.     4. Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.     5. Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.     6. Poziom ryzyka, określający istotność danej detekcji.     7. Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu). 28. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK). 29. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal). 30. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne. 31. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania. 32. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu. 33. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji. 34. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu. 35. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie. 36. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora. 37. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych, jeśli zostaną one uwzględnione w wygenerowanych detekcjach. 38. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań. 39. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres. 40. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF. 41. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi. 42. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim. 43. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji. 44. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru. 45. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR. 46. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie. 47. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransomware. 48. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI) 49. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach. 50. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny. 51. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania. 52. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami. 53. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe. 54. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików. 55. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów. 56. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem. 57. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http. 58. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania. 59. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione. 60. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego. 61. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego. 62. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta. 63. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania. 64. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca. 65. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta. 66. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera. 67. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych. 68. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie. 69. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp. 70. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego. 71. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie. 72. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym 73. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji). 74. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów. 75. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów. 76. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”, „rootkit”. 77. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne. 78. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta. 79. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku. 80. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta. 81. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger”, „dialer”, „trojan” w kwarantannie. 82. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX. 83. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania. 84. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona. 85. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach. 86. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej. 87. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http. 88. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta. 89. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych. 90. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki. 91. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn. 92. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta. 93. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW. 94. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej. 95. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS. 96. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”. 97. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów. 98. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp. 99. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn. 100. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego. 101. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup. 102. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej. 103. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji. 104. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej). 105. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora. 106. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych. 107. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV. 108. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji. 109. Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji. 110. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie. 111. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów. 112. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć. 113. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu. 114. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji. 115. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces. 116. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej. 117. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego. 118. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej. 119. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. 120. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth. 121. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej. 122. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy. 123. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu. 124. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach. 125. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego. 126. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu. 127. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker 128. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows. 129. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania. 130. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych. 131. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych. 132. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware. 133. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS) 134. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji. 135. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji. 136. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików. 137. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania. 138. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 139. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach. 140. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. 141. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware. 142. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora. 143. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora. 144. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji. 145. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji. 146. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji. 147. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku. 148. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny. 149. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN 150. Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD) 151. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej. 152. Rozwiązanie pozwala na wygenerowanie pliku za pocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop). 153. Wygenerowany plik może być otwarty i wykorzystany do zdalnego podłączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji. 154. Centralna administracja      1. Portal zarządzający jest dostępny w języku polskim.      2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.      3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.      4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.      5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.      6. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.      7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.      8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.      9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.      10. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.      11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.      12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.      13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.      14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki.      15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach dla których dana poprawka została wydana.      16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.      17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.      18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.      19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.      20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.      21. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.      22. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.      23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.      24. Profile mogą być przypisane do pojedynczych hostów lub do grup.      25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.      26. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.      27. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.      28. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.      29. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.      30. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.      31. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.      32. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.      33. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego.      34. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.      35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.      36. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji |
| **Moduł wykrywania i reagowania na podejrzanych aktywności na urządzeniach końcowych (XDR)** – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | 1. System klasy EDR/XDR zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową. 2. Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta. 3. Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej. 4. Rozwiązanie posiada możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:    1. Microsoft Windows 10    2. Microsoft Windows 11    3. MacOS 11 “Big Sur”    4. MacOS 10.15 “Catalina”    5. MacOS 10.14 “Mojave”    6. MacOS 10.15 “Catalina” 5. Rozwiązanie posiada możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:    1. Microsoft® Windows Server 2012    2. Microsoft® Windows Server 2016    3. Microsoft® Windows Server 2019    4. Microsoft® Windows Server 2022 6. Wspierane przeglądarki internetowej:    1. Microsoft Edge    2. Mozilla Firefox    3. Google Chrome    4. Safari 7. Rozwiązanie posiada polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze. 8. Oprogramowanie instalowane na stacjach końcowych i serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku. 9. Agent instalowany na stacjach końcowych i serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory. 10. Agent instalowany na stacjach końcowych i serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania. 11. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach. 12. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń. 13. Agent instalowany na stacjach końcowych i serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:     1. dostęp do pliku;     2. tworzenie nowego procesu;     3. nawiązane połączenia sieciowe;     4. wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;     5. zawartość skryptów uruchamianych na monitorowanej stacji. 14. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej. 15. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych. 16. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS. 17. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy). 18. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet. 19. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej. 20. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów. 21. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego. 22. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym. 23. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami. 24. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii. 25. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym. 26. Każda detekcja zawiera co najmniej następujące informacje:     1. Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.     2. Data i czas wystąpienia podejrzanych zdarzeń.     3. Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.     4. Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.     5. Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.     6. Poziom ryzyka, określający istotność danej detekcji.     7. Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu). 27. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK). 28. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal). 29. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne. 30. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania. 31. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu. 32. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji. 33. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu. 34. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie. 35. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora. 36. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach. 37. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań. 38. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres. 39. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF. 40. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi. 41. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim. 42. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji. 43. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru. 44. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR. 45. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie. 46. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji. 47. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu antywirusowego oraz mechanizmów zarządzania podatnościami. 48. Dodanie klucza licencyjnego skutkuje aktywowaniem dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym. |
| **Certyfikaty i standardy –** dokumenty załączyć wraz z ofertą lub na wezwanie Zamawiającego | 1. System musi posiadać certyfikaty:    1. OPSWAT (dla EDR na poziomie min. Platinium),    2. AV Comperative Advance +    3. AV-TEST (ochrona w 2023 na poziomie min.6)    4. Rozwiązanie wyróżnione przez AV-Test jako "najlepszy wykonawca" w testach Advanced EDR Test 2024 na podstawie scenariuszy cyberataków - APT18, TA577, Turla i FIN6    5. Producent systemu lub Autoryzowany Dystrybutor producenta musi posiadać certyfikat ISO 9001 oraz 27001 na świadczenie usług związanych z cyberbezpieczeństwem.    6. Producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikację ISAE 3000 assurance-based SOC 2 Type 2    7. Producent systemu lub autoryzowany dystrybutor producenta musi być aktywnym członkiem Cloud Security Alliance    8. Zespół reagowania na incydenty od producenta systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikację CREST i NCSC |
| **Rozszerzone wsparcie serwisowe** | 1. System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora **na okres do 30.06.2026 r.** 2. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:    1. Wsparcie telefoniczne zespołu certyfikowanych inżynierów.    2. Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.    3. Doradztwo w zakresie konfiguracji.    4. Zdalne wsparcie techniczne.    5. Pomoc w zakładaniu zgłoszeń serwisowych u producenta.    6. Przygotowanie do zdalnej konfiguracji.    7. Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.    8. Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.    9. Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.    10. Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. 3. **Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.** 4. Oferent winien przedłożyć dokumenty:    1. Oświadczanie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).    2. Certyfikat ISO 9001 oraz 27001 autoryzowanego podmiotu serwisującego. |

# Macierz dyskowa – 2 szt.

| **Parametr** | **Charakterystyka (wymagania minimalne) – macierz TYP 1** |
| --- | --- |
| **Procesor** | 1. Wielordzeniowy procesor o architekturze 64-bitowej. |
| **Obudowa** | 1. Typu rack o wysokości maksymalnie 2U wraz z szynami przesuwnymi umożliwiającymi montaż w szafie rack w zestawie. |
| **Pamięć RAM** | 1. Minimum 16GB DDR4 ECC UDIMM (2 x 8GB). Model pamięci musi znajdować się na oficjalnej liście zgodności producenta – nie zezwala się na stosowanie zamienników. |
| **Ilość obsługiwanych dysków** | 1. Minimum 12 dysków o maksymalnej pojemności nie mniejszej niż 18TB każdy,  po podłączeniu modułów rozszerzających minimum 24 dyski. |
| **Zainstalowane dyski** | 1. 12 dysków o pojemności 12TB każdy zgodnych z listą kompatybilności oferowanego serwera oraz charakteryzujących się następującymi parametrami:    1. prędkość obrotowa: minimum 7200 RPM,    2. gwarancja: minimum 60 miesięcy,    3. MTBF: minimum 2 miliony.    4. możliwość aktualizacji oprogramowania dysku bezpośrednio z poziomu systemu operacyjnego serwera NAS.    5. W razie awarii dysków muszą one pozostać u Zamawiającego |
| **Interfejsy sieciowe** | 1. Minimum 2 porty 1GbE RJ-45. 2. Minimum 1 port 10GbE RJ-45. 3. Minimum 2 porty 10GbE SFP+. 4. Obsługa agregacji łączy. |
| **Porty** | 1. Minimum 2 porty USB 3.2. Minimum 1 gniazdo rozszerzenia służące do podłączania jednostek rozszerzających. |
| **Wskaźniki LED** | 1. Status, HDD, zasilanie, LAN |
| **Obsługa RAID** | 1. Podstawowy, RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare. |
| **Funkcje RAID** | 1. Możliwość zwiększania pojemności poprzez wymianę dysków na większe. Migracja poziomu RAID w trybie online dla minimum RAID 1 i RAID 5. |
| **Szyfrowanie** | 1. Możliwość szyfrowania wybranych udziałów sieciowych. |
| **Protokoły** | 1. SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP |
| **Usługi** | 1. Serwer VPN, Serwer pocztowy, Stacja monitoringu, Windows ACL, Integracja z Windows Active Directory, Firewall, Serwer plików, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Usługa DDNS, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki (min. 65 tys. w cały systemie), możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów. 2. Wykonywanie kopii zapasowych maszyn wirtualnych ze środowisk takich jak VMware vSphere, VMware free ESXi oraz Microsoft Hyper-V 2016 i 2019 (wraz z klastrami przełączania awaryjnego) z wykorzystaniem centralnego panelu zarządzania oraz dodatkowo:    1. Obsługa wszystkich typów i wersji sprzętu wirtualnego VMware, w tym 62TB VMDK.    2. Obsługa maszyn wirtualnych Hyper-V generacji 1 i 2, w tym dysków VHDX o pojemności 64 TB i wersji sprzętu wirtualnego od 5.0 do 9.0.    3. W przypadku tworzenia kopii zapasowych Microsoft Hyper-V wymagany jest wolumin systemowy hosta z co najmniej 512 MB wolnego miejsca w celu zainstalowania narzędzia do przenoszenia danych.    4. Kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym konfiguracji danych i systemu.    5. Kopia zapasowa bez agentów.    6. Korzystanie z funkcji VMware Changed Block Tracking i funkcji Hyper-V Resilient Change Tracking do wykonywania przyrostowej kopii zapasowej    7. Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowych.    8. Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów i natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V lub wbudowanego wirtualizatora na serwerze NAS.    9. W przypadku przywracania na poziomie plików w systemie operacyjnym gościa obsługiwane systemy plików systemu Windows to NTFS i FAT32, a obsługiwane systemy plików systemu Linux to NTFS, FAT32, ext3, I ext4.    10. Kopia zapasowa uwzględniające aplikacje dla maszyn wirtualnych VMware vSphere lub Microsoft Hyper-V działających w systemie Microsoft Windows 2003 SP1 lub nowszym (z wyjątkiem Nano Server z powodu braku architektury VSS).    11. Obsługa tworzenia kopii zapasowych systemów operacyjnych i aplikacji obsługiwanych przez rozwiązania VMware vSphere i Microsoft Hyper-V. 3. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klaster obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora. |
| **Obsługa migawek** | 1. Liczba migawek folderu współdzielonego: minimum 1000 |
| **Zarządzanie dyskami** | 1. SMART, sprawdzanie złych sektorów. |
| **Język GUI** | 1. Polski |
| **Gwarancja i serwis** | 1. Minimum 36 miesięcy gwarancji producenta. |
| **Waga bez dysków** | 1. Maksymalnie 15 kg |
| **Typowy pobór mocy podczas pracy** | 1. Maksymalnie 130W |
| **Certyfikaty** | 1. CE, FCC |
| **System plików** | 1. Dyski wewnętrzne: BTRFS |
| **Szyfrowanie** | 1. Mechanizm szyfrowania sprzętowego |
| **Zasilacz** | 1. Redundantny zasilacz o mocy minimum 300W. |
| **Chłodzenie** | 1. Minimum 3 wentylatory z możliwością regulowania prędkości obrotowej oraz wymiany w urządzeniu podczas pracy. |

# Oprogramowanie NAC - Network Access Control

1. **Opis funkcjonalności rozwiązania**
   1. Wymagane jest dostarczenie rozwiązania typu NAC (Network Access Control), służącego do monitorowania sieci lokalnych w celu uwidocznienia pracujących w nich urządzeń oraz wykrywania nowych urządzeń pojawiających się w sieci, w czasie rzeczywistym. Rozwiązanie musi raportować aktualny stan każdego urządzenia, z uwzględnieniem takich atrybutów, jak adres MAC, adres IP, nazwa hosta, system operacyjny, itp., pozyskując te informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.).
   2. Rozwiązanie ma za zadanie zapewnić, aby tylko urządzenia, których aktualny stan spełnia zdefiniowaną przez administratora politykę bezpieczeństwa, mogły bez ograniczeń ze strony NAC pracować w sieci lokalnej. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenia, których aktualny stan nie spełnia danych warunków polityki bezpieczeństwa (np. nowe, po raz pierwszy pojawiające się urządzenie lub stacja robocza z wyłączonym oprogramowaniem antywirusowym). Mechanizm kwarantanny powinien umożliwiać całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym, jak również blokowanie częściowe, w zakresie definiowanym przez administratora (przez wskazanie adresów IP, z którymi urządzenie może się komunikować). Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej.
   3. Rozwiązanie musi posiadać funkcjonalność typu Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów.
2. **Wymagania ogólne rozwiązania NAC**
   1. Ma zapewnić widoczność i monitorowanie wszystkich urządzeń pracujących w sieci lokalnej oraz powiadamiać o nowych urządzeniach pojawiających się w sieci.
   2. Musi zapewniać automatyczne blokowanie komunikacji sieciowej między nowym, niezaufanym urządzeniem a zaufanymi, zarządzanymi urządzeniami pracującymi w sieci.
   3. Musi umożliwiać sprawdzanie statusu aktualizacji oprogramowania antywirusowego i poprawek systemowych na zarządzanych stacjach roboczych Windows i w przypadku nie spełniania określonych wymagań, automatycznie ograniczać tym stacjom roboczym możliwość pracy w sieci.
   4. Musi umożliwiać odbieranie komunikatów bezpieczeństwa z innych systemów bezpieczeństwa (np. firewalla) i automatyczne blokowanie na tej podstawie wskazanych urządzeń w sieci.
   5. Musi mieć funkcję wykrywania faktu skanowania urządzeń i portów wykonywanego przez urządzenie w sieci lokalnej i automatycznie blokować takie urządzenie, aby zapobiegać potencjalnemu szerzeniu się malware.
   6. Stosowany mechanizm blokowania musi wykorzystywać protokół ARP i działać całkowicie niezależnie od innych elementów infrastruktury sieciowej.
   7. Rozwiązanie musi działać bezagentowo, bez konieczności instalowania jakichkolwiek agentów na urządzeniach w sieci oraz bez konieczności dokonywania zmian w infrastrukturze sieciowej.
   8. Rozwiązanie musi umożliwiać wysyłanie alertów do administratora za pomocą e-maila oraz SMS
   9. Rozwiązanie musi być zarządzane przez interfejs webowy, obsługiwany przeglądarką internetową
   10. Wymaga się, aby rozwiązanie było dostarczone w postaci maszyny wirtualnej na platformę VMware oraz Hyper-V. System musi pozwalać na monitorowanie co najmniej 10 sieci VLAN i monitorowanie łącznie co najmniej 300 urządzeń.
   11. Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej i dostarczone z licencją pozwalającą na monitorowanie 125 urządzeń wraz ze wsparciem technicznym na okres 2 lat.
3. **Wymagania szczegółowe – monitorowanie podsieci**
   1. Rozwiązanie musi w czasie rzeczywistym raportować widoczność wszystkich urządzeń pracujących w monitorowanych podsieciach.
   2. Rozwiązanie musi wykrywać nowe nieznane urządzenie, dołączające się do sieci LAN lub WLAN, w czasie nie dłuższym, niż 5 sekund oraz wysyłać powiadomienie mailowe do administratora
   3. Rozwiązanie musi wykrywać przypadki skanowania urządzeń i portów w monitorowanych podsieciach i blokować urządzenie inicjujące takie skanowanie
   4. Rozwiązanie musi posiadać funkcję pułapki sieciowej (honeypot), symulującą w każdej monitorowanej podsieci standardowe usługi sieciowe, co najmniej: ssh, telnet, ftp i smb. Rozwiązanie musi rejestrować każdą próbę zalogowania się do takiej symulowanej usługi, zapisując użytą nazwę użytkownika, hasło użytkownika i źródłowy MAC/IP.
   5. Rozwiązanie musi określać aktualny stan każdego urządzenia, pozyskując informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.) oraz odświeżać te informacje cyklicznie. Musi być możliwość wykorzystania pozyskanych informacji do definiowania polityk bezpieczeństwa.
   6. Rozwiązanie musi chronić przed podszywaniem się pod adres MAC (MAC spoofing), umożliwiając zdefiniowanie „odcisku palca” (fingerprint) dla każdego zaufanego urządzenia. Odcisk palca musi być kombinacją co najmniej: adresu MAC, adresu IP, nazwy hosta, nazwy systemu operacyjnego, otwartych portów TCP. Jeśli przeprowadzana cyklicznie weryfikacja odcisku palca wykaże jego zmianę, urządzenie powinno zostać zablokowane.
   7. Rozwiązanie musi obsługiwać VLANy, tj. umożliwiać monitorowanie przez jeden fizyczny interfejs sieciowy wielu podsieci, zdefiniowanych jako VLANy
4. **Wymagania szczegółowe – polityka bezpieczeństwa**
   1. Rozwiązanie musi umożliwiać definiowanie polityki bezpieczeństwa, czyli określenie przez administratora, jakie warunki musi spełniać aktualny stan urządzenia, aby uzyskało ono określony dostęp do sieci.
   2. W definiowaniu polityki bezpieczeństwa musi być możliwość wykorzystania informacji o aktualnym stanie urządzenia, pozyskanych bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.), poprzez integrację z tymi systemami.
   3. Polityka bezpieczeństwa musi umożliwiać przypisanie do urządzenia jednego z trzech trybów dostępu do sieci:
      1. pełny dostęp
      2. blokowanie (całkowity brak dostępu)
      3. ograniczony dostęp
   4. Zakres ograniczonego dostępu powinien być definiowany przez administratora, np. w postaci list ACL, określających, do których adresów IP i portów urządzenie ma dostęp. Musi być możliwość zdefiniowania wielu różnych zakresów ograniczonego dostępu.
   5. Rozwiązanie powinno automatycznie sprawdzać, które warunki polityki bezpieczeństwa spełnia urządzenie i na tej podstawie przypisywać do urządzenia właściwy zakres dostępu.
   6. Zakres dostępu, wynikający ze spełnienia przez urządzenie danych warunków polityki bezpieczeństwa powinien być egzekwowany przez mechanizm kwarantanny.
   7. Musi być możliwość łatwego, manualnego tworzenie białej listy adresów MAC, czyli listy urządzeń mogących bez żadnych ograniczeń ze strony NAC pracować w sieci.
5. **Wymagania szczegółowe – mechanizm kwarantanny**
   1. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenie, aby wyegzekwować ograniczenia dostępu do sieci, wynikające z polityki bezpieczeństwa
   2. Mechanizm kwarantanny powinien umożliwiać:
      1. całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym,
      2. częściowe blokowanie komunikacji urządzenia z otoczeniem sieciowym, w zakresie definiowanym przez administratora przez wskazanie adresów IP i portów, z którymi urządzenie może się komunikować
   3. Mechanizm kwarantanny powinien blokować komunikację urządzenia w czasie nie dłuższym, niż 5 sekund od zaistnienia warunku, powodującego nałożenie kwarantanny
   4. Dla urządzeń zaufanych, czyli w polityce bezpieczeństwa spełniających kryteria pełnego dostępu do sieci, rozwiązanie nie powinno w żaden sposób przekierowywać ani blokować komunikacji wychodzącej z tych urządzeń
   5. Kwarantanna powinna być zdejmowana z urządzenia automatycznie, gdy spełni ono kryteria polityki bezpieczeństwa, pozwalające na pełny dostęp
   6. Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej, musi być niezależny od stosowanych w sieci przełączników, zarządzalnych bądź niezarządzalnych
   7. Awaria rozwiązania nie może powodować blokady komunikacji w sieci, tj. w przypadku awarii rozwiązania wszystkie urządzenia mają mieć pełny dostęp do sieci
   8. Rozwiązanie musi umożliwiać włączenie i wyłączenie mechanizmu kwarantanny (blokowania komunikacji) w każdej monitorowanej podsieci osobno
6. **Wymagania szczegółowe – integracja z systemami zewnętrznymi**
   1. Rozwiązanie musi umieć sprawdzić, czy urządzenia z systemem Windows są dołączone do domeny AD
   2. Rozwiązanie powinno umożliwiać sprawdzanie statusu oprogramowania antywirusowego, poprawek systemowych i firewalla bezpośrednio na zarządzanych stacjach roboczych Windows w domenie AD, w sposób bezagentowy, przy użyciu WMI.
   3. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym poprawkami Windows i sprawdzanie statusu zainstalowanych poprawek na zarządzanych urządzeniach z systemem Windows. Wymagana jest możliwość integracji co najmniej z systemami: Microsoft WSUS.
   4. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym agentami antywirusowymi i sprawdzanie statusu agentów AV zainstalowanych na zarządzanych urządzeniach (co najmniej, czy agent jest zainstalowany, aktywny i ma aktualne sygnatury wirusów). Wymagana jest możliwość integracji co najmniej z systemami: Bitdefender, Carbon Black, CrowdStrike, Cybereason, Eset, FireEye, McAfee, SentinelOne, Sophos, Symantec, TrendMicro, Webroot.
   5. Rozwiązanie musi umożliwiać wykorzystanie pozyskanych informacji, wymienionych w poprzedzających punktach 1-4, do definiowania polityki bezpieczeństwa.
   6. Rozwiązanie musi umieć odbierać alerty przysyłane za pomocą e-mail lub syslog z innych urządzeń bezpieczeństwa (np. firewalla) i na podstawie zawartych w nich informacji blokować wskazane podejrzane urządzenie
7. **Wymagania szczegółowe – rejestracja urządzeń zewnętrznych: pracowników, gości i konsultantów (Captive Portal)**
   1. Rozwiązanie musi posiadać wbudowaną funkcję Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów. NAC musi przekierowywać ruch HTTP/S od nieznanych urządzeń do tego portalu.
   2. Captive Portal musi umożliwiać pracownikom rejestrowanie urządzeń prywatnych (BYOD) i wnioskowanie o dostęp do sieci w ograniczonym zakresie, zdefiniowanym przez administratora.
   3. Przy rejestracji przez pracowników ich prywatnych urządzeń, Captive Portal powinien umożliwiać użycie ich kont Active Directory
   4. Powinna istnieć możliwość ograniczenia ilości i rodzaju rejestrowanych przez pracownika prywatnych urządzeń
   5. Powinna być możliwość przypisania ograniczonego dostępu dla zarejestrowanych urządzeń prywatnych
   6. Captive Portal musi umożliwiać osobom nie będącym pracownikami (gościom lub konsultantom) wnioskowanie o ograniczony dostęp do sieci
   7. W przypadku rejestracji urządzeń gości powinna być możliwość rejestracji samodzielnie przez gościa oraz przez uprawnionego pracownika firmy
   8. Zarejestrowane urządzenia gości powinny automatycznie tracić przydzielony dostęp po upływie zdefiniowanego czasu
   9. Powinna istnieć możliwość ograniczenia ilości urządzeń rejestrowanych przez gościa
   10. Dla zarejestrowanych urządzeń gości powinna być możliwość ograniczenia, w jakich przedziałach czasu i z jakich podsieci będą one miały dostęp do sieci
   11. Dla urządzeń gości powinna być możliwość przypisania dostępu ograniczonego tylko do dostępu do internetu
   12. Dla urządzeń konsultantów powinna być możliwość przypisania dostępu ograniczonego do wybranych zasobów lokalnych
   13. Rozwiązanie musi umożliwiać zatwierdzenie dostępu dla zarejestrowanego urządzenia gościa i konsultanta drogą mailową. Osoba zatwierdzająca powinna otrzymać z systemu e-mail z wnioskiem o dostęp i udzielić go, odpowiadając na maila lub klikając przygotowany link w treści maila.
   14. Rozwiązanie musi przechowywać historyczne raporty dostępu do sieci użytkowników typu gość i konsultant
   15. Wygląd Captive Portal musi być edytowalny w zakresie co najmniej zmiany firmowego logo i kolorów oraz informacji, jakie we wniosku rejestracyjnym musi podać gość lub konsultant
8. **Pozostałe wymagania** 
   1. Rozwiązanie powinno oferować uwierzytelnianie administratora za pomocą dodatkowego faktora, oprócz hasła (2FA).
   2. Rozwiązanie powinno oferować możliwość zainstalowania opcjonalnego agenta na zarządzanych stacjach roboczych (wymagane wsparcie dla Windows, Linux i MacOS), który przesyła do serwera zarządzającego NAC szczegółowe informacje na temat stacji roboczej, umożliwiając definiowanie na bazie tych informacji precyzyjnych polityk bezpieczeństwa.
   3. Rozwiązanie nie powinno pogarszać wydajności pracy przełączników i routerów, nie może wymagać współpracy z przełącznikami przez port mirroring czy port spanning.
   4. Rozwiązanie nie powinno pogarszać wydajność łącz WAN
   5. Rozwiązanie nie powinno pogarszać wydajności pracy monitorowanych urządzeń w sieci
9. **Usługi**
   1. Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, w wymienionym poniżej zakresie, przeprowadzoną przez wykwalikowanego inżyniera, certyfikowanego przez producenta rozwiązania:
      1. instalacja i konfiguracja rozwiązania w maszynie wirtualnej na platformie Zamawiającego
      2. szkolenie dla administratora rozwiązania
      3. wsparcie w języku polskim w trybie 8x5 w dni robocze
      4. kwartalny przegląd konfiguracji rozwiązania
   2. Wymaga się, aby dostawca przedstawił:
      1. oświadczenie producenta o posiadaniu przez dostawcę kwalifikacji technicznych, niezbędnych do wykonania wdrożenia oferowanego rozwiązania i szkolenia
      2. osobowy certyfikat inżynierski pracownika, który będzie wykonywał wdrożenie