

## Spis treści

1. SERWER TYP I – 2 szt.....	2
2. SERWER TYP II – 1 szt.....	27
3. ACCESS POINT– 7 SZT.....	53
4. PRZEŁACZNIK TYP I.....	55
5. PRZEŁACZNIK TYP II.....	58
6. PRZEŁACZNIK TYP III.....	61
7. PRZEŁACZNIK TYP IV – SZT. 3 .....	64
8. PRZEŁACZNIK TYP V – SZT. 2 .....	67
9. FIREWALL SPRZĘTOWY – 1 SZT.....	70
10. NAS TYP I – 1 SZT.....	82
11. DYSKI DO NAS TYP I – 12 SZT. ....	87
12. NAS TYP II – 1 SZT.....	87
13. OPROGRAMOWANIE DO ARCHIWIZACJI LOGÓW -1 LICENCJA URZĄD -1 LICENCJA OPS.....	89
14. OPROGRAMOWANIE DO TWORZENIA KOPII ZAPASOWYCH NA POTRZEBY URZĘDU .....	90
15. OPROGRAMOWANIE DO TWORZENIA KOPII ZAPASOWYCH NA POTRZEBY OPS.....	92
16. DYSKI DO MACIERZY - 14 SZT.....	93
17. WDROŻENIE .....	94
OKABLOWANIE .....	94

## 1. SERWER TYP I – 2 szt

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1.	Charakterystyka ogólna	<ul style="list-style-type: none"> <li>Serwer będzie kluczowym elementem infrastruktury IT Zamawiającego, przeznaczonym do instalacji oraz uruchomienia oprogramowania służącego podniesieniu poziomu cyberbezpieczeństwa. Serwer będzie wspierać działanie różnorodnych narzędzi dedykowanych ochronie sieci oraz zarządzaniu bezpieczeństwem, m.in. takich jak: Zakup i wdrożenie oprogramowania do kategoryzacji i archiwizacji logów – narzędzie do gromadzenia, analizowania i przechowywania logów z infrastruktury IT.</li> </ul>	<b>Producent:</b>  <b>Model wersja:</b>  SPEŁNIA TAK /NIE
2.	Obudowa	<ul style="list-style-type: none"> <li>Obudowa Rack o wysokości 2U</li> <li>12 wnęk na dyski 3.5"</li> <li>Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej</li> <li>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.</li> </ul>	SPEŁNIA TAK /NIE
3.	Płyta główna	<ul style="list-style-type: none"> <li>Płyta główna z możliwością zainstalowania do dwóch procesorów.</li> <li>Obsługa procesorów 32 rdzeniowych.</li> <li>Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.</li> <li>Na płycie głównej powinno znajdować się 16 slotów przeznaczonych do instalacji pamięci.</li> <li>Płyta główna powinna obsługiwać do 1TB pamięci RAM.</li> </ul>	SPEŁNIA TAK /NIE
4.	Chipset	<ul style="list-style-type: none"> <li>Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych</li> </ul>	SPEŁNIA TAK /NIE
5.	Procesor	<ul style="list-style-type: none"> <li>Zainstalowane dwa procesory klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 238 w teście SPECrate2017_int_base, dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> dla konfiguracji dwuprocessorowej.</li> </ul>	SPEŁNIA TAK /NIE
6.	RAM	<ul style="list-style-type: none"> <li>384GB DDR5 RDIMM 5600MT/s,</li> </ul>	SPEŁNIA TAK /NIE
7.	Kontroler RAID	<ul style="list-style-type: none"> <li>Sprzętowy kontroler dyskowy, posiadający               <ul style="list-style-type: none"> <li>Min. 8GB nieulotnej pamięci cache,</li> <li>Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.</li> <li>Wsparcie dla dysków samoszyfrujących</li> </ul> </li> </ul>	SPEŁNIA TAK /NIE
8.	Dyski twarde	<ul style="list-style-type: none"> <li>Zainstalowane:               <ul style="list-style-type: none"> <li>1x dysk SSD SATA o pojemności min. 480GB, Hot-Plug</li> </ul> </li> </ul>	SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.</li> </ul>	
9.	Gniazda PCI	<ul style="list-style-type: none"> <li>Cztery sloty PCIe</li> </ul>	SPEŁNIA TAK /NIE
10.	Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> <li>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)</li> <li>Dwuportowa karta sieciowa 10Gb Ethernet w standardzie BaseT</li> <li>Dwuportowa karta 32Gb FC</li> </ul>	SPEŁNIA TAK /NIE
11.	Wbudowane porty	<ul style="list-style-type: none"> <li>4 porty USB w tym min: <ul style="list-style-type: none"> <li>1 port USB 3.0 z tyłu obudowy,</li> <li>1 port micro USB z przodu obudowy</li> </ul> </li> <li>2 port VGA z czego jeden z przodu obudowy</li> <li>Możliwość rozbudowy o port RS232</li> </ul>	SPEŁNIA TAK /NIE
12.	Video	<ul style="list-style-type: none"> <li>Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024</li> </ul>	SPEŁNIA TAK /NIE
13.	Wentylatory	<ul style="list-style-type: none"> <li>Redundantne, Hot-Plug</li> </ul>	SPEŁNIA TAK /NIE
14.	Zasilacze	<ul style="list-style-type: none"> <li>Redundantne, Hot-Plug min. 1100W klasy Titanium</li> </ul>	SPEŁNIA TAK /NIE
15.	Elementy montażowe	<ul style="list-style-type: none"> <li>Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych</li> <li>Ramię (organizator) do kabli ułatwiające wysuwanie serwera do celów serwisowych</li> </ul>	SPEŁNIA TAK /NIE
16.	System operacyjny/dodatki oprogramowanie	<ul style="list-style-type: none"> <li>Windows Server 2025 Standard – <b>licencja dobrana tak, aby przy oferowanych procesorach umożliwić uruchomienie 4 maszyn wirtualnych.</b></li> <li>Microsoft Windows Server 2025 Standard lub równoważny spełniający min. poniższe wymagania:</li> <li>Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.</li> <li>Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.</li> <li>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.</li> <li>Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.</li> <li>Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.</li> <li>Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</li> <li>Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.</li> <li>Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;</li> <li>Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</li> </ul>	<p><b>Producent</b></p> <p><b>Nazwa i wersja oprogramowania</b></p> <p>SPEŁNIA TAK /NIE</p>

		<ul style="list-style-type: none"> <li>Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agencję rządową zajmującą się bezpieczeństwem informacji.</li> <li>Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.</li> <li>Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.</li> <li>Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</li> <li>Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.</li> <li>Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.</li> <li>Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play).</li> <li>Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</li> <li>Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).</li> <li>Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</li> <li>Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</li> <li>Możliwość migracji konfiguracji systemu Microsoft Windows Serwer 2012/2016.</li> </ul>	
17.	<b>Bezpieczeństwo</b>	<ul style="list-style-type: none"> <li>Zatrask górnej pokrywki oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.</li> <li>Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</li> <li>BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła</li> <li>Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</li> <li>Moduł TPM 2.0</li> <li>Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera</li> <li>Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem</li> <li>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).</li> </ul>	SPEŁNIA TAK /NIE
18.	<b>Karta Zarządzania</b>	<ul style="list-style-type: none"> <li>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: <ul style="list-style-type: none"> <li>zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</li> <li>zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);</li> <li>szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;</li> <li>możliwość podmontowania zdalnych wirtualnych napędów;</li> <li>wirtualną konsolę z dostępem do myszy, klawiatury;</li> <li>wsparcie dla IPv6;</li> </ul> </li> </ul>	SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>o wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;</li> <li>o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;</li> <li>o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;</li> <li>o integracja z Active Directory;</li> <li>o możliwość obsługi przez dwóch administratorów jednocześnie;</li> <li>o wsparcie dla automatycznej rejestracji DNS</li> <li>o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.</li> <li>o możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera</li> <li>o możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera</li> </ul> <p>oraz z możliwością rozszerzenia funkcjonalności o:</p> <ul style="list-style-type: none"> <li>o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej</li> <li>o Przesyłanie danych telemetrycznych w czasie rzeczywistym</li> <li>o Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze</li> <li>o Automatyczna rejestracja certyfikatów (ACE)</li> </ul>	
19.	<b>Oprogramowanie do zarządzania</b> – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	<p>Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</p> <ul style="list-style-type: none"> <li>• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych</li> <li>• integracja z Active Directory</li> <li>• Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta</li> <li>• Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish</li> <li>• Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram</li> <li>• Szczegółowy opis wykrytych systemów oraz ich komponentów</li> <li>• Możliwość eksportu raportu do CSV, HTML, XLS, PDF</li> <li>• Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.</li> <li>• Grupowanie urządzeń w oparciu o kryteria użytkownika</li> <li>• Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji</li> <li>• Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach</li> <li>• Szybki podgląd stanu środowiska</li> <li>• Podsumowanie stanu dla każdego urządzenia</li> <li>• Szczegółowy status urządzenia/elementu/komponentu</li> <li>• Generowanie alertów przy zmianie stanu urządzenia.</li> <li>• Filtry raportów umożliwiające podgląd najważniejszych zdarzeń</li> <li>• Integracja z service desk producenta dostarczonej platformy sprzętowej</li> <li>• Możliwość przejęcia zdalnego pulpitu</li> <li>• Możliwość podmontowania wirtualnego napędu</li> <li>• Kreator umożliwiający dostosowanie akcji dla wybranych alertów</li> <li>• Możliwość importu plików MIB</li> </ul>	<p>Producent:</p> <p>Nawa i wersja:</p> <p>SPEŁNIA TAK /NIE</p>

- Przesyłanie alertów „as-is” do innych konsol firm trzecich
- Możliwość definiowania ról administratorów
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
- Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
- Zdalne uruchamianie diagnostyki serwera.
- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
  - Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

**20. Oprogramowanie do monitorowania**  
– w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania

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:

- Monitoring:
  - ilość podłączonych oraz rozłączonych systemów
  - stan podłączonych urządzeń
  - informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów
  - Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia
  - informacje o statusie gwarancji dla poszczególnych urządzeń
  - informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń
  - informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.
  - Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych

**Producent:**

**Nawa i wersja:**

SPEŁNIA TAK /NIE

- Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.
- Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.
- Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.
- Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.
- Monitoring parametrów serwerów z informacją o minimum:
  - Obciążeniu procesora
  - Zużyciu pamięci RAM
  - Temperaturze procesorów
  - Temperaturze powietrza wlotowego
  - Zużyciu prądu
  - Zmianach w fizycznej konfiguracji serwera
  - Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Monitoring parametrów pamięci masowych z informacją o minimum:
  - Opóźnieniach
  - IOPS
  - Przepustowości
  - Utylizacji kontrolerów
  - Pojemności całkowita i dostępna
  - Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.
  - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
  - Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
  - Informacje o poziomie redukcji danych
  - Informacje o statusie replikacji oraz snapshotów
- Monitoring parametrów przełączników sieciowych z informacją o minimum:
  - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
  - Stanie komponentów: zasilacze, wentylatory
  - Podłączonych hostach
  - Ilości i statusu portów
  - Utylizacji procesora
  - Utylizacji poszczególnych portów
  - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.

- Aktualizacja firmware

- możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
- możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
- możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania
- możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
- możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania
- Raporty
  - Możliwość generowania raportów dla serwerów zawierających informację o:
    - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
    - Średnim obciążeniu: procesorów, pamięci RAM, IO,
  - Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:
    - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji
  - Generowanie raportów do plików CSV i PDF
- Cyberbezpieczeństwo
  - Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.
  - Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.
  - Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.
  - Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.
- Wspierane urządzenia
  - Urządzenie Producenta dostarczane w ramach postępowania
  - Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)
- Wirtualny asystent

		<ul style="list-style-type: none"> <li>○ 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;</li> <li>• Możliwość rozszerzenia funkcjonalności <ul style="list-style-type: none"> <li>○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.</li> </ul> </li> <li>• Inne <ul style="list-style-type: none"> <li>○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android</li> </ul> </li> <li>• Certyfikaty <ul style="list-style-type: none"> <li>○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami: <ul style="list-style-type: none"> <li>▪ ISO 27001</li> <li>▪ NIST Security and Privacy Controls for Federal Information Systems and Organization</li> </ul> </li> <li>○ CSA Cloud Control Matrix</li> </ul> </li> </ul>	
21.	Certyfikaty	<ul style="list-style-type: none"> <li>• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001</li> <li>• Serwer musi posiadać deklaracja CE.</li> <li>• 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 <a href="http://www.epeat.net">www.epeat.net</a> potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - <b>Wykonawca złoży dokument potwierdzający spełnianie wymogu.</b></li> <li>• 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.</li> </ul>	SPEŁNIA TAK /NIE
22.	Dokumentacja użytkownika	<ul style="list-style-type: none"> <li>• Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</li> <li>• Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</li> </ul>	SPEŁNIA TAK /NIE
23.	Wsparcie techniczne i oprogramowanie – w formularzu oferty należy podać pełną nazwę	<p>Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego, automatycznie tworzące zgłoszenia serwisowe w przypadku awarii. Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera.</p>	<p><b>Producent:</b></p> <p><b>Nawa i wersja:</b></p> <p>SPEŁNIA TAK /NIE</p>

	oferowanego oprogramowania	<p>Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów.</p> <p>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.</p> <p>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.</p> <p>Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :</p> <ul style="list-style-type: none"> <li>• Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień.</li> <li>• Predykcja analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów.</li> <li>• Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta.</li> <li>• upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,</li> <li>• 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 :             <ol style="list-style-type: none"> <li>a. o poprawkach i usprawnieniach dotyczących aktualizacji</li> <li>b. dacie wydania ostatniej aktualizacji</li> <li>c. priorytecie aktualizacji</li> <li>d. zgodność z systemami operacyjnymi</li> <li>e. jakiego komponentu sprzętu dotyczy aktualizacja</li> <li>f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.</li> </ol> </li> <li>• wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne</li> <li>• możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.</li> <li>• - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty ( dd-mm-rrrr )</li> <li>• sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą ( dd-mm-rrrr ) i wersją ( rewizja wydania )</li> <li>• dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml</li> <li>• raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiem jakich komponentów to dotyczyło,</li> </ul>	
--	----------------------------	--	--

		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.	
24.	Warunki gwarancji	<ul style="list-style-type: none"> <li>• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres minimum 36 -m-cy.</li> <li>• Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.</li> <li>• Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.</li> <li>• Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</li> <li>• 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.</li> <li>• Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</li> <li>• 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.</li> <li>• 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.</li> <li>• Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: <ul style="list-style-type: none"> <li>○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.</li> <li>○ 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.</li> <li>○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.</li> <li>○ 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.</li> <li>○ 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</li> </ul> </li> </ul>	SPEŁNIA TAK /NIE

		<p>do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.</p> <ul style="list-style-type: none"> <li>Wymagane dołączenie do oferty dokumentu potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Dokument potwierdzony przez Producenta oferowanego rozwiązania</li> <li>Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.</li> </ul>	
25.	<p><b>Ochrona serwerów</b> –</p> <p>w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania</p>	<p><b>Ochrona antywirusowa 8 licencji</b> niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.</p> <p>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.</p> <p>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.</p> <p>Rozwiązanie dla ochrony antywirusowej systemów serwerowych wspiera następujące systemy operacyjne:</p> <ul style="list-style-type: none"> <li>Microsoft Windows Server 2016</li> <li>Microsoft Windows Server 2019</li> <li>Microsoft Windows Server 2022</li> </ul> <p>Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:</p> <ul style="list-style-type: none"> <li>Microsoft Edge</li> <li>Mozilla Firefox</li> <li>Google Chrome</li> <li>Safari</li> </ul> <p>Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:</p> <p>Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika.</p> <p>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.</p> <p>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</p> <ol style="list-style-type: none"> <li>Oprogramowanie instalowane na serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.</li> <li>Agent instalowany na serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.</li> <li>Agent instalowany na serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.</li> </ol>	<p><b>Producent:</b></p> <p><b>Nazwa i wersja oprogramowania</b></p>

4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na serwerach .
5. Dane zebrane przez agenta instalowanego na serwerach są przysyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.
6. Agent instalowany na serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:
  - dostęp do pliku;
  - tworzenie nowego procesu;
  - nawiązane połączenia sieciowe;
  - wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
  - zawartość skryptów uruchamianych na monitorowanej stacji.
7. 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.
8. Dane zbierane przez agenta instalowanego na serwerach , przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łącz sieciowych.
9. Komunikacja agentów instalowanych na stacjach roboczych, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
10. Komunikacja agentów instalowanych na stacjach roboczych, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
11. 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.
12. Dane zbierane przez agentów na serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych.
14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na serwerach w środowisku informatycznym.
16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
17. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
18. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
19. Każda detekcja zawiera co najmniej następujące informacje:
  - Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.

- Data i czas wystąpienia podejrzanych zdarzeń.
  - Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.
  - Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
  - Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
  - Poziom ryzyka, określający istotność danej detekcji.
  - Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).
20. 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).
  21. 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).
  22. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
  23. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
  24. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
  25. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
  26. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
  27. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
  28. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
  29. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
  30. 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.
  31. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
  32. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
  33. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
  34. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
  35. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.

36. 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.
37. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
38. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim połączeniu oraz aktualnym statusie.
39. 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.
40. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
41. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
42. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
43. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
44. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
45. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
46. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
47. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
48. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
49. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
50. 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.
51. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
52. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
53. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.
54. 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.

55. 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.
56. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
57. 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.
58. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
59. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
60. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
61. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
62. 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.
63. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
64. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
65. 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).
66. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
67. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
68. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit”.
69. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.
70. 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.
71. 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.
72. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejranych plików do dodatkowej analizy przez producenta.
  73. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.
  74. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
  75. 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.
  76. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
  77. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
  78. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
  79. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
  80. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
  81. 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.
  82. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamianie skryptów ActiveX i pobierane pliki.
  83. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
  84. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
  85. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.
  86. Użytkownik podczas próby przejścia na witrynę znajdującą się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
  87. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
  88. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.
  89. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
  90. 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.

91. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
92. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
93. 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.
94. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
95. 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.
96. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
97. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
98. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
99. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
100. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
101. Moduł aktualizacji aplikacji pełni rolę mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
102. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
103. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
104. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
105. 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.
106. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
107. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.

- 108.Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
- 109.Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
- 110.System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
- 111.Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
- 112.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.
- 113.Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
- 114.Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
- 115.Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
- 116.Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
- 117.Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.
- 118.Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
- 119.Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker
- 120.Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.
- 121.W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.
- 122.Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.
- 123.Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.
- 124.Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.
- 125.Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)
- 126.W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.
- 127.Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.
- 128.Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.

- |  |  |  |
|--|--|--|
|  | <p>129.Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.</p> <p>130.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.</p> <p>131.Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.</p> <p>132.Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.</p> <p>133.Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.</p> <p>134.Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.</p> <p>135.Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.</p> <p>136.Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.</p> <p>137.Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji.</p> <p>138.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.</p> <p>139.Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.</p> <p>140.Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.</p> <p>141.Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN</p> <p>142.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)</p> <p>143.Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.</p> <p>144.Rozwiązanie pozwala na wygenerowanie pliku za pomocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop).</p> <p>145.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.</p> |  |
|--|--|--|

## 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 powiadomienia 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 połączenia 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 dawać 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.
- W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji

26.	<b>Moduł wykrywania i reagowania na podejrzanych aktywności na urządzeniach końcowych (XDR) – w formularzu</b>	<p><b>System klasy EDR/XDR – 8 licencji</b> zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.</p> <p>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.</p>	<p><b>Producent</b></p> <p><b>Nazwa i wersja oprogramowania</b></p>
-----	--	---	---

	<p>oferty należy podać pełną nazwę oferowanego oprogramowania</p>	<p>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.</p> <p>Rozwiązanie posiada możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows 10</li> <li>• Microsoft Windows 11</li> <li>• MacOS 11 "Big Sur"</li> <li>• MacOS 10.15 "Catalina"</li> <li>• MacOS 10.14 "Mojave"</li> <li>• MacOS 10.15 "Catalina"</li> </ul> <p>Rozwiązanie posiada możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:</p> <ul style="list-style-type: none"> <li>• Microsoft® Windows Server 2012</li> <li>• Microsoft® Windows Server 2016</li> <li>• Microsoft® Windows Server 2019</li> <li>• Microsoft® Windows Server 2022</li> </ul> <p>Wspierane przeglądarki internetowe:</p> <ul style="list-style-type: none"> <li>• Microsoft Edge</li> <li>• Mozilla Firefox</li> <li>• Google Chrome</li> <li>• Safari</li> </ul> <p>Rozwiązanie posiada polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze.</p> <ol style="list-style-type: none"> <li>1. Oprogramowanie instalowane na serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.</li> <li>2. Agent instalowany na serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.</li> <li>3. Agent instalowany na serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.</li> <li>4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na serwerach.</li> <li>5. Dane zebrane przez agenta instalowanego na serwerach są przysyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.</li> <li>6. Agent instalowany na serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń: <ul style="list-style-type: none"> <li>• dostęp do pliku;</li> <li>• tworzenie nowego procesu;</li> <li>• nawiązane połączenia sieciowe;</li> <li>• wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;</li> <li>• zawartość skryptów uruchamianych na monitorowanej stacji.</li> </ul> </li> <li>7. 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.</li> </ol>	<p>SPEŁNIA TAK /NIE</p>
--	---	--	-------------------------

8. Dane zbierane przez agenta instalowanego na serwerach, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łącz sieciowych.
9. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
10. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
11. 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.
12. Dane zbierane przez agentów na serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.
14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na serwerach w środowisku informatycznym.
16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
17. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
18. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
19. Każda detekcja zawiera co najmniej następujące informacje:
  - Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
  - Data i czas wystąpienia podejrzanych zdarzeń.
  - Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.
  - Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
  - Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
  - Poziom ryzyka, określający istotność danej detekcji.
  - Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).
20. 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).

21. 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).
22. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
23. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
24. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
25. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
26. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
27. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
28. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
29. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
30. 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.
31. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
32. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
33. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
34. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
35. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
36. 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.
37. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
38. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim połączeniu oraz aktualnym statusie.

39. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.

40. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu antywirusowego oraz mechanizmów zarządzania podatnościami.

41. Dodanie klucza licencyjnego skutkuje aktywowaniem dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.

Dla zapewnienia wysokiego poziomu usług **podmiot udzielający wsparcia technicznego dla oprogramowania musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług serwisowych 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. (dokumenty załączyć do oferty).

**Oferent winien przedłożyć dokumenty:**

Oświadczenie Producenta oprogramowania lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).

Certyfikat ISO 9001 oraz 27001 podmiotu serwisującego.

## 2. SERWER TYP II – 1 szt

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1.	Charakterystyka ogólna	<ul style="list-style-type: none"> <li>Serwer będzie kluczowym elementem infrastruktury IT Zamawiającego, przeznaczonym do instalacji oraz uruchomienia oprogramowania służącego podniesieniu poziomu cyberbezpieczeństwa. Serwer będzie wspierać działanie różnorodnych narzędzi dedykowanych ochronie sieci oraz zarządzaniu bezpieczeństwem, m.in. takich jak: Zakup i wdrożenie oprogramowania do kategoryzacji i archiwizacji logów – narzędzie do gromadzenia, analizowania i przechowywania logów z infrastruktury IT.</li> </ul>	<b>Producent:</b>  <b>Model wersja:</b>  SPEŁNIA TAK /NIE
2.	Obudowa	<ul style="list-style-type: none"> <li>Obudowa Rack o wysokości 2U</li> <li>12 wnęk na dyski 3.5"</li> <li>Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej</li> <li>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.</li> </ul>	SPEŁNIA TAK /NIE
3.	Płyta główna	<ul style="list-style-type: none"> <li>Płyta główna z możliwością zainstalowania do dwóch procesorów.</li> <li>Obsługa procesorów 32 rdzeniowych.</li> <li>Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.</li> <li>Na płycie głównej powinno znajdować się 16 slotów przeznaczonych do instalacji pamięci.</li> <li>Płyta główna powinna obsługiwać do 1TB pamięci RAM.</li> </ul>	SPEŁNIA TAK /NIE
4.	Chipset	<ul style="list-style-type: none"> <li>Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych</li> </ul>	SPEŁNIA TAK /NIE
5.	Procesor	<ul style="list-style-type: none"> <li>Zainstalowane dwa procesory, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 169 w teście SPECrate2017_int_base, dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> dla konfiguracji dwuprocesorowej.</li> </ul>	SPEŁNIA TAK /NIE
6.	RAM	<ul style="list-style-type: none"> <li>128GB DDR5 RDIMM 5600MT/s,</li> </ul>	SPEŁNIA TAK /NIE
7.	Kontroler RAID	<ul style="list-style-type: none"> <li>Sprzętowy kontroler dyskowy, posiadający               <ul style="list-style-type: none"> <li>Min. 8GB nieulotnej pamięci cache,</li> <li>Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.</li> <li>Wsparcie dla dysków samoszyfrujących</li> </ul> </li> </ul>	SPEŁNIA TAK /NIE
8.	Dyski twarde	<ul style="list-style-type: none"> <li>Zainstalowane:               <ul style="list-style-type: none"> <li>8x dysk SSD SATA 6Gbps o pojemności min. 1.92TB, Hot-Plug</li> </ul> </li> </ul>	SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.</li> </ul>	
9.	Gniazda PCI	<ul style="list-style-type: none"> <li>Sześć slotów PCIe</li> </ul>	SPEŁNIA TAK /NIE
10.	Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> <li>Wbudowane min. 4 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)</li> </ul>	SPEŁNIA TAK /NIE
11.	Wbudowane porty	<ul style="list-style-type: none"> <li>4 porty USB w tym min: <ul style="list-style-type: none"> <li>1 port USB 3.0 z tyłu obudowy,</li> <li>1 port micro USB z przodu obudowy</li> </ul> </li> <li>2 port VGA z czego jeden z przodu obudowy</li> <li>Możliwość rozbudowy o port RS232</li> </ul>	SPEŁNIA TAK /NIE
12.	Video	<ul style="list-style-type: none"> <li>Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024</li> </ul>	SPEŁNIA TAK /NIE
13.	Wentylatory	<ul style="list-style-type: none"> <li>Redundantne, Hot-Plug</li> </ul>	SPEŁNIA TAK /NIE
14.	Zasilacze	<ul style="list-style-type: none"> <li>Redundantne, Hot-Plug min. 700W klasy Titanium</li> </ul>	SPEŁNIA TAK /NIE
15.	Elementy montażowe	<ul style="list-style-type: none"> <li>Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych</li> <li>Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych</li> </ul>	SPEŁNIA TAK /NIE
16.	System operacyjny/dodatkowe oprogramowanie	<ul style="list-style-type: none"> <li>Windows Server 2025 Standard – <b>licencja dobrana tak, aby przy oferowanych procesorach umożliwić uruchomienie 4 maszyn wirtualnych.</b></li> <li>Microsoft Windows Server 2025 Standard lub równoważny spełniający min. poniższe wymagania:</li> <li>Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.</li> <li>Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.</li> <li>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.</li> <li>Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.</li> <li>Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.</li> <li>Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</li> <li>Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.</li> <li>Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;</li> <li>Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</li> <li>Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.</li> </ul>	SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>• Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.</li> <li>• Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilkoma serwerami.</li> <li>• Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</li> <li>• Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.</li> <li>• Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.</li> <li>• Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play).</li> <li>• Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</li> <li>• Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).</li> <li>• Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</li> <li>• Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</li> <li>• Możliwość migracji konfiguracji systemu Microsoft Windows Serwer 2021/2016.</li> </ul>	
17.	Bezpieczeństwo	<ul style="list-style-type: none"> <li>• Zatrzaśnięcie górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardej.</li> <li>• Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</li> <li>• BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła</li> <li>• Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</li> <li>• Moduł TPM 2.0</li> <li>• Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera</li> <li>• Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem</li> <li>• 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).</li> </ul>	SPEŁNIA TAK /NIE
18.	Karta Zarządzania	<ul style="list-style-type: none"> <li>• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: <ul style="list-style-type: none"> <li>○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</li> <li>○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);</li> </ul> </li> </ul>	SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>o szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;</li> <li>o możliwość podmontowania zdalnych wirtualnych napędów;</li> <li>o wirtualną konsolę z dostępem do myszy, klawiatury;</li> <li>o wsparcie dla IPv6;</li> <li>o wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;</li> <li>o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;</li> <li>o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;</li> <li>o integracja z Active Directory;</li> <li>o możliwość obsługi przez dwóch administratorów jednocześnie;</li> <li>o wsparcie dla automatycznej rejestracji DNS</li> <li>o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.</li> <li>o możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera</li> <li>o możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: <ul style="list-style-type: none"> <li>o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej</li> <li>o Przesyłanie danych telemetrycznych w czasie rzeczywistym</li> <li>o Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze</li> <li>o Automatyczna rejestracja certyfikatów (ACE)</li> </ul> </li> </ul>	
19.	<b>Oprogramowanie do zarządzania</b> – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	<p>Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</p> <ul style="list-style-type: none"> <li>• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych</li> <li>• integracja z Active Directory</li> <li>• Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta</li> <li>• Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish</li> <li>• Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram</li> <li>• Szczegółowy opis wykrytych systemów oraz ich komponentów</li> <li>• Możliwość eksportu raportu do CSV, HTML, XLS, PDF</li> <li>• Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.</li> <li>• Grupowanie urządzeń w oparciu o kryteria użytkownika</li> <li>• Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji</li> <li>• Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach</li> <li>• Szybki podgląd stanu środowiska</li> <li>• Podsumowanie stanu dla każdego urządzenia</li> </ul>	<p><b>Producent:</b></p> <p><b>Nawa i wersja:</b></p> <p>SPEŁNIA TAK /NIE</p>

		<ul style="list-style-type: none"> <li>• Szczegółowy status urządzenia/elementu/komponentu</li> <li>• Generowanie alertów przy zmianie stanu urządzenia.</li> <li>• Filtry raportów umożliwiające podgląd najważniejszych zdarzeń</li> <li>• Integracja z service desk producenta dostarczonej platformy sprzętowej</li> <li>• Możliwość przejęcia zdalnego pulpitu</li> <li>• Możliwość podmontowania wirtualnego napędu</li> <li>• Kreator umożliwiający dostosowanie akcji dla wybranych alertów</li> <li>• Możliwość importu plików MIB</li> <li>• Przesyłanie alertów „as-is” do innych konsol firm trzecich</li> <li>• Możliwość definiowania ról administratorów</li> <li>• Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów</li> <li>• Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)</li> <li>• Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta</li> <li>• Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów</li> <li>• Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.</li> <li>• Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.</li> <li>• Wdrażanie serwerów, rozwiązań modułowych oraz przełączników sieciowych w oparciu o profile</li> <li>• Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.</li> <li>• Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.</li> <li>• Zdalne uruchamianie diagnostyki serwera.</li> <li>• Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. <ul style="list-style-type: none"> <li>◦ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.</li> </ul> </li> </ul>	
20.	<b>Oprogramowanie do monitorowania</b> – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	<p>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:</p> <ul style="list-style-type: none"> <li>• Monitoring: <ul style="list-style-type: none"> <li>◦ ilość podłączonych oraz rozłączonych systemów</li> <li>◦ stan podłączonych urządzeń</li> <li>◦ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów</li> </ul> </li> </ul>	<p><b>Producent:</b></p> <p><b>Nawa i wersja:</b></p> <p>SPEŁNIA TAK/NIE</p>

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

- Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
  - Informacje o poziomie redukcji danych
  - Informacje o statusie replikacji oraz snapshotów
- Monitoring parametrów przełączników sieciowych z informacją o minimum:
  - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
  - Stanie komponentów: zasilacze, wentylatory
  - Podłączonych hostach
  - Ilości i statusu portów
  - Utylizacji procesora
  - Utylizacji poszczególnych portów
  - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Aktualizacja firmware
  - możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
  - możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania
- Raporty
  - Możliwość generowania raportów dla serwerów zawierających informację o:
    - Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
    - Średnim obciążeniu: procesorów, pamięci RAM, IO,
  - Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:
    - Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji
  - Generowanie raportów do plików CSV i PDF

		<ul style="list-style-type: none"> <li>• Cyberbezpieczeństwo             <ul style="list-style-type: none"> <li>○ 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.</li> <li>○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.</li> <li>○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.</li> <li>○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.</li> </ul> </li> <li>• Wspierane urządzenia             <ul style="list-style-type: none"> <li>○ Urządzenie Producenta dostarczane w ramach postępowania</li> <li>○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)</li> </ul> </li> <li>• Wirtualny asystent             <ul style="list-style-type: none"> <li>○ 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;</li> </ul> </li> <li>• Możliwość rozszerzenia funkcjonalności             <ul style="list-style-type: none"> <li>○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.</li> </ul> </li> <li>• Inne             <ul style="list-style-type: none"> <li>○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android</li> </ul> </li> <li>• Certyfikaty             <ul style="list-style-type: none"> <li>○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami:                 <ul style="list-style-type: none"> <li>▪ ISO 27001</li> <li>▪ NIST Security and Privacy Controls for Federal Information Systems and Organization</li> </ul> </li> <li>○ CSA Cloud Control Matrix</li> </ul> </li> </ul>	
21.	Certyfikaty	<ul style="list-style-type: none"> <li>• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001</li> <li>• Serwer musi posiadać deklarację CE.</li> <li>• 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</li> </ul>	SPEŁNIA TAK /NIE

		<p>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 <a href="http://www.epeat.net">www.epeat.net</a> potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - <b>Wykonawca złoży dokument potwierdzający spełnianie wymogu.</b></p> <ul style="list-style-type: none"> <li>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.</li> </ul>	
22.	<b>Dokumentacja użytkownika</b>	<ul style="list-style-type: none"> <li>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</li> <li>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</li> </ul>	SPEŁNIA TAK /NIE
23.	<b>Wsparcie techniczne i oprogramowanie</b> – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	<p>Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego, automatycznie tworzące zgłoszenia serwisowe w przypadku awarii. Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera.</p> <p>Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów.</p> <p>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.</p> <p>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.</p> <p>Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :</p> <ul style="list-style-type: none"> <li>Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień.</li> <li>Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów.</li> <li>Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta.</li> <li>upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,</li> </ul>	<p><b>Producent:</b></p> <p><b>Nawa i wersja:</b></p> <p>SPEŁNIA TAK /NIE</p>

		<ul style="list-style-type: none"> <li>• 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 : <ul style="list-style-type: none"> <li>a. o poprawkach i usprawnieniach dotyczących aktualizacji</li> <li>b. dacie wydania ostatniej aktualizacji</li> <li>c. priorytecie aktualizacji</li> <li>d. zgodność z systemami operacyjnymi</li> <li>e. jakiego komponentu sprzętu dotyczy aktualizacja</li> <li>f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.</li> </ul> </li> <li>• wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne</li> <li>• możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.</li> <li>• - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty ( dd-mm-rrrr )</li> <li>• sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą ( dd-mm-rrrr ) i wersją ( rewizja wydania )</li> <li>• dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml</li> <li>• raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiorem 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.</li> </ul>	
24.	Warunki gwarancji	<ul style="list-style-type: none"> <li>• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres minimum 36 m-cy.</li> <li>• Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.</li> <li>• Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.</li> <li>• Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</li> <li>• 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.</li> <li>• Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</li> </ul>	SPEŁNIA TAK/NIE

		<ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li><li>• Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:<ul style="list-style-type: none"><li>○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.</li><li>○ 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.</li><li>○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.</li><li>○ 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.</li><li>○ 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 przekaze 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.</li></ul></li><li>• Dołączenie do oferty dokumentu potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Dokument potwierdzony przez Producenta oferowanego rozwiązania,</li><li>• Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.</li></ul>	
25.	Ochrona serwerów – w formularzu oferty	Ochrona antywirusowa 8 licencji: niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się	Producent:

## na Rozwój Cyfrowy

	należy podać pełną nazwę oferowanego oprogramowania	<p>na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.</p> <p>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.</p> <p>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.</p> <p>Rozwiązanie dla ochrony antywirusowej systemów serwerowych wspiera następujące systemy operacyjne:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows Server 2016</li> <li>• Microsoft Windows Server 2019</li> <li>• Microsoft Windows Server 2022</li> </ul> <p>Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:</p> <ul style="list-style-type: none"> <li>• Microsoft Edge</li> <li>• Mozilla Firefox</li> <li>• Google Chrome</li> <li>• Safari</li> </ul> <p>Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:</p> <p>Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika.</p> <p>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.</p> <p>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</p> <ol style="list-style-type: none"> <li>1. Oprogramowanie instalowane na serwerach , zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.</li> <li>2. Agent instalowany na serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.</li> <li>3. Agent instalowany na serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.</li> <li>4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na serwerach .</li> <li>5. Dane zebrane przez agenta instalowanego na serwerach są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.</li> </ol>	Nazwa i wersja oprogramowania
--	---	---	-------------------------------

6. Agent instalowany na serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:
  - dostęp do pliku;
  - tworzenie nowego procesu;
  - nawiązane połączenia sieciowe;
  - wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
  - zawartość skryptów uruchamianych na monitorowanej stacji.
7. 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.
8. Dane zbierane przez agenta instalowanego na serwerach, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.
9. Komunikacja agentów instalowanych na stacjach roboczych, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
10. Komunikacja agentów instalowanych na stacjach roboczych, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
11. 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.
12. Dane zbierane przez agentów na serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych.
14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na serwerach w środowisku informatycznym.
16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
17. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
18. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
19. Każda detekcja zawiera co najmniej następujące informacje:
  - Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
  - Data i czas wystąpienia podejrzanych zdarzeń.
  - Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.

- Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
  - Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
  - Poziom ryzyka, określający istotność danej detekcji.
  - Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).
20. 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).
  21. 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).
  22. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
  23. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
  24. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
  25. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
  26. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrótnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
  27. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
  28. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
  29. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
  30. 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.
  31. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
  32. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.

33. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
34. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
35. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
36. Rozwiązanie umożliwia wyszukiwanie 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.
37. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
38. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim połączeniu oraz aktualnym statusie.
39. 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.
40. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
41. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
42. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
43. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
44. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
45. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
46. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
47. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
48. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
49. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
50. 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.

51. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
52. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
53. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.
54. 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.
55. 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.
56. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
57. 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.
58. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
59. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
60. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
61. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
62. 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.
63. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
64. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
65. 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).
66. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
67. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.

68. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit”.
69. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.
70. 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.
71. 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.
72. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
73. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.
74. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
75. 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.
76. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
77. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
78. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
79. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
80. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
81. 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.
82. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamianie skryptów ActiveX i pobierane pliki.

83. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
84. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
85. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.
86. Użytkownik podczas próby przejścia na witrynę znajdującą się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
87. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
88. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.
89. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
90. 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.
91. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
92. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
93. 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.
94. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
95. 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.
96. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
97. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
98. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
99. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
100. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.

101. Moduł aktualizacji aplikacji pełni rolę mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
102. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
103. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
104. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
105. 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.
106. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
107. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
108. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
109. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
110. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
111. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
112. 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.
113. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
114. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
115. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
116. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
117. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.

118. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
119. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker
120. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.
121. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.
122. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.
123. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.
124. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.
125. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)
126. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.
127. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.
128. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.
129. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.
130. 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.
131. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.
132. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
133. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.
134. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
135. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
136. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.

137. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezauważanych aplikacji.
138. Istnieje możliwość 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.
139. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.
140. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.
141. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN.
142. 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).
143. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.
144. Rozwiązanie pozwala na wygenerowanie pliku za pomocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop).
145. 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.

#### Centralna administracja

36. Portal zarządzający jest dostępny w języku polskim.
37. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
38. 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.
39. Interfejs zarządzania posiada funkcję wyświetlania monitorów o zbliżającym się zakończeniu licencji, a także powiadomienia o zakończeniu licencji.
40. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
41. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
42. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do

		<p>ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.</p> <p>43. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.</p> <p>44. 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.</p> <p>45. 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.</p> <p>46. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.</p> <p>47. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.</p> <p>48. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.</p> <p>49. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki.</p> <p>50. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach dla których dana poprawka została wydana.</p> <p>51. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.</p> <p>52. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.</p> <p>53. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.</p> <p>54. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.</p> <p>55. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.</p> <p>56. 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.</p> <p>57. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.</p> <p>58. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.</p> <p>59. Profile mogą być przypisane do pojedynczych hostów lub do grup.</p> <p>60. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.</p>	
--	--	---	--

		<p>61. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.</p> <p>62. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.</p> <p>63. 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.</p> <p>64. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.</p> <p>65. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.</p> <p>66. Tworzone profile muszą dawać administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.</p> <p>67. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.</p> <p>68. 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.</p> <p>69. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.</p> <p>70. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.</p> <p>W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji</p>	
26.	<p><b>Moduł wykrywania i reagowania na podejrzanych aktywności na urządzeniach końcowych (XDR) – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania</b></p>	<p><b>System klasy EDR/XDR 8 licencji</b> : zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.</p> <p>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.</p> <p>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.</p> <p>Rozwiązanie posiada możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:</p>	<p><b>Producent</b></p> <p><b>Nazwa i wersja oprogramowania</b></p> <p>SPEŁNIA TAK /NIE</p>

- Microsoft Windows 10
- Microsoft Windows 11
- MacOS 11 "Big Sur"
- MacOS 10.15 "Catalina"
- MacOS 10.14 "Mojave"
- MacOS 10.15 "Catalina"

Rozwiązanie posiada możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:

- Microsoft® Windows Server 2012
- Microsoft® Windows Server 2016
- Microsoft® Windows Server 2019
- Microsoft® Windows Server 2022

Wspierane przeglądarki internetowe:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

Rozwiązanie posiada polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze.

1. Oprogramowanie instalowane na serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.
2. Agent instalowany na serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.
3. Agent instalowany na serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.
4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na serwerach.
5. Dane zebrane przez agenta instalowanego na serwerach są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.
6. Agent instalowany na serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:
  - dostęp do pliku;
  - tworzenie nowego procesu;
  - nawiązane połączenia sieciowe;
  - wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
  - zawartość skryptów uruchamianych na monitorowanej stacji.
7. 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.
8. Dane zbierane przez agenta instalowanego na serwerach, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łącz sieciowych.

9. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
10. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
11. 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.
12. Dane zbierane przez agentów na serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.
14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na serwerach w środowisku informatycznym.
16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
17. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
18. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
19. Każda detekcja zawiera co najmniej następujące informacje:
  - Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
  - Data i czas wystąpienia podejrzanych zdarzeń.
  - Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.
  - Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
  - Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
  - Poziom ryzyka, określający istotność danej detekcji.
  - Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).
20. 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).

21. 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).
22. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
23. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
24. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
25. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
26. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
27. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
28. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
29. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
30. 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.
31. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
32. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
33. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
34. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
35. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
36. 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.

		<p>37. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.</p> <p>38. 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.</p> <p>39. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.</p> <p>40. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu antywirusowego oraz mechanizmów zarządzania podatnościami.</p> <p>41. Dodanie klucza licencyjnego skutkuje aktywowaniem dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.</p> <p>Dla zapewnienia wysokiego poziomu usług <b>podmiot udzielający wsparcia technicznego dla oprogramowania musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług serwisowych oraz usług związanych z cyberbezpieczeństwem</b>. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. (dokumenty załączyć do oferty).</p> <p><b>Oferent winien przedłożyć dokumenty:</b>  Oświadczenie Producenta oprogramowania lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).  Certyfikat ISO 9001 oraz 27001 podmiotu serwisującego.</p>	
--	--	--	--

### 3. ACCESS POINT– 7 SZT.

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1.	Charakterystyka	<p>Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.</p> <ol style="list-style-type: none"> <li>Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych: <ol style="list-style-type: none"> <li>Temperatura 0–50°C,</li> <li>Wilgotność 5–90%.</li> </ol> </li> <li>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.</li> <li>Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać co najmniej następujące standardy:</li> </ol>	<p><b>Producent</b></p> <p><b>Model /wersja</b></p> <p>SPEŁNIA TAK /NIE</p>

- |  |  |  |
|--|--|--|
|  | <ul style="list-style-type: none"> <li>a. 2.4 GHz 802.11b/g/n,</li> <li>b. 5 GHz 802.11a/n/ac/ax,</li> <li>c. 6 GHz 802.11ax/be</li> </ul> <ul style="list-style-type: none"> <li>4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.</li> <li>5. Urządzenie musi być wyposażone w moduł BLE.</li> <li>6. Urządzenie musi być wyposażone w co najmniej jeden interfejs Ethernet (RJ45) wspierający co najmniej szybkości 1G/2.5G/5.0G.</li> <li>7. 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.</li> <li>8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych: <ul style="list-style-type: none"> <li>a. Tunnel,</li> <li>b. Bridge,</li> <li>c. Mesh.</li> </ul> </li> <li>9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.</li> <li>10. 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).</li> <li>11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje: <ul style="list-style-type: none"> <li>a. MIMO – 2x2,</li> <li>b. Wymagana maksymalna przepustowość dla poszczególnych modułów radiowych: <ul style="list-style-type: none"> <li>i. 688 Mbps;</li> <li>ii. 2882 Mbps;</li> <li>iii. 5765 Mbps;</li> </ul> </li> <li>c. Wymagana moc nadawania: <ul style="list-style-type: none"> <li>i. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;</li> <li>ii. min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;</li> <li>iii. min. 22 dBm dla pasma 6GHz z możliwością zmiany co 1dBm</li> </ul> </li> <li>d. Wsparcie dla kanałów 20/40/80/160/320MHz,</li> </ul> </li> </ul> |  |
|--|--|--|

		<p>e. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5dBi dla pasma 6GHz.</p> <p>f. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy.</p> <p>g. Każdy z modułów radiowych musi posiadać możliwość pracy jako dedykowany skaner.</p> <p>12. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512</p> <p>13. Funkcje dodatkowe:</p> <ul style="list-style-type: none"> <li>a. OFDMA UL i DL</li> <li>b. Spatial Reuse (BSS Coloring)</li> <li>c. UL-MU-MIMO</li> <li>d. DL-MU-MIMO</li> <li>e. Enhanced Target Wake Time (TWT)</li> <li>f. Wbudowany analizator widma</li> <li>g. Wbudowane mechanizmy WIPS/WIDS</li> </ul>	
2.	<b>Gwarancja oraz wsparcie</b>	Urządzenie musi mieć zapewnioną dożywną ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 36 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.	SPEŁNIA TAK /NIE

#### 4. PRZEŁĄCZNIK TYP I

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1.	Charakterystyka ogólna	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych	<b>Producent</b>  <b>Model i wersja</b>
2.	Parametry fizyczne platformy	<ul style="list-style-type: none"> <li>• Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.</li> <li>• Zasilanie AC 230V.</li> <li>• Wbudowany redundantny zasilacz.</li> <li>• Maksymalny pobór mocy: 50 W.</li> <li>• Minimalny zakres temperatury pracy: 0-50°C.</li> </ul>	SPEŁNIA TAK /NIE
3.	Interfejsy sieciowe - wymagania minimalne	<p>1. Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:</p> <ul style="list-style-type: none"> <li>a) 48 porty GE RJ-45.</li> <li>e) 4 porty 10 GE SFP+.</li> </ul>	SPEŁNIA TAK /NIE
4.	Zarządzanie	<ul style="list-style-type: none"> <li>• Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania.</li> </ul>	SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>• Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.</li> <li>• Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).</li> <li>• Wsparcie dla SNMP w wersjach 1-3</li> <li>• Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.</li> <li>• Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.</li> <li>• Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.</li> <li>• Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).</li> <li>• Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.</li> <li>• Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.</li> <li>• Automatycznie wykonywane rewizje konfiguracji.</li> </ul>	
5.	Parametry wydajnościowe	<ul style="list-style-type: none"> <li>• Przepustowość urządzenia - min. 176 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 260 Mpps.</li> <li>• Tablica adresów MAC o pojemności co najmniej 32 k wpisów.</li> <li>• Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.</li> </ul>	SPEŁNIA TAK /NIE
6.	Wymagane funkcje	<ul style="list-style-type: none"> <li>• Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.</li> <li>• Obsługa Jumbo Frames.</li> <li>• Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).</li> <li>• Agregacja portów zgodna ze standardem 802.3ad.</li> <li>• Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.</li> <li>• Wsparcie dla Private VLAN.</li> <li>• Obsługa routingu statycznego.</li> <li>• Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP.</li> <li>• Port-mirroring.</li> <li>• Uwierzytelnianie 802.1x na poziomie portu.</li> <li>• Uwierzytelnianie 802.1x w oparciu o adres MAC.</li> <li>• W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).</li> <li>• W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.</li> <li>• W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.</li> <li>• Obsługa protokołu sFlow.</li> </ul>	
7.	Dodatkowe funkcje urządzenia przy integracji z systemem	<ol style="list-style-type: none"> <li>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-</li> </ol>	SPEŁNIA TAK /NIE

## na Rozwój Cyfrowy

	centralnego zarządzania / NAC	<p>leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:</p> <ul style="list-style-type: none"> <li>• Centralne zarządzanie konfiguracją urządzenia</li> <li>• Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania</li> <li>• Centralne zarządzanie sieciami VLAN.</li> <li>• Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u</li> <li>• Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..</li> <li>• Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.</li> <li>• 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.</li> <li>• Automatyczna detekcja i rekomendacje konfiguracji.</li> <li>• Przesyłanie logów na zewnętrzny serwer syslog.</li> <li>• Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.</li> <li>• Obsługa białych i czarnych list adresów MAC.</li> <li>• Wykrywanie aplikacji komunikujących się w sieci.</li> </ul> <p>2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.</p> <p>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.</p>	
8.	Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	<ul style="list-style-type: none"> <li>• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.</li> <li>• System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.</li> </ul>	SPEŁNIA TAK /NIE
9.	Gwarancja oraz wsparcie	1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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.	SPEŁNIA TAK /NIE
10.	Rozszerzone wsparcie serwisowe	<p>1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym Dniu Roboczym /w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy.</p> <p>2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać <b>certyfikat ISO 9001</b> w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku</p>	SPEŁNIA TAK /NIE

		<p>polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. Oferent winien przedłożyć dokumenty:</p> <ul style="list-style-type: none"> <li>Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).</li> <li>Certyfikat ISO 9001 podmiotu serwisującego.</li> </ul>	
11.	Opisy do wymagań ogólnych	<p>1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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.</p> <p>2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań</p>	SPEŁNIA TAK /NIE

## 5. PRZEŁĄCZNIK TYP II

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1.	Charakterystyka ogólna	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych	<b>Producent</b>  <b>Model i wersja</b>
2.	Parametry fizyczne platformy	<ul style="list-style-type: none"> <li>Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.</li> <li>Zasilanie AC 230V.</li> <li>Budżet mocy dla portów PoE min.: 370 W.</li> <li>Maksymalny pobór mocy bez budżetu dla PoE: 110 W.</li> <li>Minimalny zakres temperatury pracy: 0-40°C.</li> </ul>	SPEŁNIA TAK /NIE
3.	Interfejsy sieciowe - wymagania minimalne	<p>2. Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:</p> <p>a) 48 porty GE RJ-45.</p> <p>W tym porty PoE w ilości co najmniej: 24, zgodne ze standardem: 802.3af oraz 802.3at.</p>	SPEŁNIA TAK /NIE

		b) 4 porty 10 GE SFP+.	
4.	Zarządzanie	<ul style="list-style-type: none"> <li>Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).</li> <li>Wsparcie dla SNMP w wersjach 1-3</li> <li>Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.</li> <li>Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.</li> <li>Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.</li> <li>Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).</li> <li>Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.</li> <li>Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.</li> <li>Automatycznie wykonywane rewizje konfiguracji.</li> </ul>	SPEŁNIA TAK /NIE
5.	Parametry wydajnościowe	<ul style="list-style-type: none"> <li>Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.</li> <li>Tablica adresów MAC o pojemności co najmniej 32k wpisów.</li> <li>Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.</li> </ul>	SPEŁNIA TAK /NIE
6.	Wymagane funkcje	<ul style="list-style-type: none"> <li>Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.</li> <li>Obsługa Jumbo Frames.</li> <li>Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).</li> <li>Agregacja portów zgodna ze standardem 802.3ad.</li> <li>Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.</li> <li>Obsługa routingu statycznego.</li> <li>Port-mirroring.</li> <li>Uwierzytelnianie 802.1x na poziomie portu.</li> <li>Uwierzytelnianie 802.1x w oparciu o adres MAC.</li> <li>W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).</li> <li>W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.</li> <li>W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.</li> <li>Obsługa protokołu sFlow.</li> </ul>	
7.	Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	<p>4. 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:</p> <ul style="list-style-type: none"> <li>Centralne zarządzanie konfiguracją urządzenia</li> </ul>	SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>• Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania</li> <li>• Centralne zarządzanie sieciami VLAN.</li> <li>• Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u</li> <li>• Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..</li> <li>• Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.</li> <li>• 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.</li> <li>• Automatyczna detekcja i rekomendacje konfiguracji.</li> <li>• Przesyłanie logów na zewnętrzny serwer syslog.</li> <li>• Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.</li> <li>• Obsługa białych i czarnych list adresów MAC.</li> <li>• Wykrywanie aplikacji komunikujących się w sieci.</li> </ul> <p>5. Musi być możliwe redundantne połączenie z elementami zarządzającymi.</p> <p>6. 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.</p>	
8.	Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	<ul style="list-style-type: none"> <li>• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.</li> <li>• System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.</li> </ul>	SPEŁNIA TAK /NIE
9.	Gwarancja oraz wsparcie	1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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.	SPEŁNIA TAK /NIE
10.	Rozszerzone wsparcie serwisowe	<p>3. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym Dniu Roboczym /w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy.</p> <p>4. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać <b>certyfikat ISO 9001</b> w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5 . Oferent winien przedłożyć dokumenty:</p>	SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).</li> <li>Certyfikat ISO 9001 podmiotu serwisującego.</li> </ul>	
12.	Opisy do wymagań ogólnych	<ol style="list-style-type: none"> <li>W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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.</li> <li>Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań</li> </ol>	SPEŁNIA TAK /NIE

## 6. PRZEŁĄCZNIK TYP III

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1.	Charakterystyka ogólna	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych	<b>Producent</b> <b>Model i wersja</b>
2.	Parametry fizyczne platformy	<ul style="list-style-type: none"> <li>Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.</li> <li>Zasilanie AC 230V.</li> <li>Budżet mocy dla portów PoE min.: 185 W.</li> <li>Maksymalny pobór mocy bez budżetu dla PoE: 55 W.</li> <li>Minimalny zakres temperatury pracy: 0-40°C.</li> </ul>	SPEŁNIA TAK /NIE
3.	Interfejsy sieciowe - wymagania minimalne	<ol style="list-style-type: none"> <li>Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:               <ol style="list-style-type: none"> <li>24 porty GE RJ-45.</li> </ol> </li> <li>W tym porty PoE w ilości co najmniej: 12, zgodne ze standardem: 802.3af oraz 802.3at.               <ol style="list-style-type: none"> <li>4 porty 10 GE SFP+.</li> </ol> </li> </ol>	SPEŁNIA TAK /NIE
4.	Zarządzanie	<ul style="list-style-type: none"> <li>Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).</li> </ul>	SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>• Wsparcie dla SNMP w wersjach 1-3</li> <li>• Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.</li> <li>• Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.</li> <li>• Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.</li> <li>• Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).</li> <li>• Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.</li> <li>• Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.</li> <li>• Automatycznie wykonywane rewizje konfiguracji.</li> </ul>	
5.	Parametry wydajnościowe	<ul style="list-style-type: none"> <li>• Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps.</li> <li>• Tablica adresów MAC o pojemności co najmniej 32k wpisów.</li> <li>• Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.</li> </ul>	SPEŁNIA TAK /NIE
6.	Wymagane funkcje	<ul style="list-style-type: none"> <li>• Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.</li> <li>• Obsługa Jumbo Frames.</li> <li>• Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).</li> <li>• Agregacja portów zgodna ze standardem 802.3ad.</li> <li>• Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.</li> <li>• Obsługa routingu statycznego.</li> <li>• Port-mirroring.</li> <li>• Uwierzytelnianie 802.1x na poziomie portu.</li> <li>• Uwierzytelnianie 802.1x w oparciu o adres MAC.</li> <li>• W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).</li> <li>• W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.</li> <li>• W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.</li> <li>• Obsługa protokołu sFlow.</li> </ul>	
7.	Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	<p>7. 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:</p> <ul style="list-style-type: none"> <li>• Centralne zarządzanie konfiguracją urządzenia</li> <li>• Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania</li> <li>• Centralne zarządzanie sieciami VLAN.</li> </ul>	SPEŁNIA TAK /NIE

## na Rozwój Cyfrowy

		<ul style="list-style-type: none"> <li>• Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u</li> <li>• Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..</li> <li>• Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.</li> <li>• 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.</li> <li>• Automatyczna detekcja i rekomendacje konfiguracji.</li> <li>• Przesyłanie logów na zewnętrzny serwer syslog.</li> <li>• Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.</li> <li>• Obsługa białych i czarnych list adresów MAC.</li> <li>• Wykrywanie aplikacji komunikujących się w sieci.</li> </ul> <p>8. Musi być możliwe redundantne połączenie z elementami zarządzającymi.</p> <p>9. 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.</p>	
8.	Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	<ul style="list-style-type: none"> <li>• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.</li> <li>• System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.</li> </ul>	SPEŁNIA TAK /NIE
9.	Gwarancja oraz wsparcie	1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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.	SPEŁNIA TAK /NIE
10.	Rozszerzone wsparcie serwisowe	<p>5. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym Dniu Roboczym /w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy.</p> <p>6. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać <b>certyfikat ISO 9001</b> w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. Oferent winien przedłożyć dokumenty:</p>	SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).</li> <li>Certyfikat ISO 9001 podmiotu serwisującego.</li> </ul>	
13.	Opisy do wymagań ogólnych	<ol style="list-style-type: none"> <li>W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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.</li> <li>Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań</li> </ol>	SPEŁNIA TAK /NIE

## 7. PRZEŁĄCZNIK TYP IV – SZT. 3

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1.	Charakterystyka ogólna	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych	<b>Producent</b>  <b>Model i wersja</b>
2.	Parametry fizyczne platformy	<ul style="list-style-type: none"> <li>Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.</li> <li>Zasilanie AC 230V.</li> <li>Maksymalny pobór mocy: 30 W.</li> <li>Minimalny zakres temperatury pracy: 0-40°C.</li> </ul>	SPEŁNIA TAK /NIE
3.	Interfejsy sieciowe - wymagania minimalne	<ol style="list-style-type: none"> <li>Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:               <ol style="list-style-type: none"> <li>24 porty GE RJ-45</li> <li>4 porty 10 GE SFP+</li> </ol> </li> </ol>	SPEŁNIA TAK /NIE
4.	Zarządzanie	<ul style="list-style-type: none"> <li>Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).</li> <li>Wsparcie dla SNMP w wersjach 1-3</li> </ul>	SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.</li> <li>Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.</li> <li>Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.</li> <li>Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).</li> <li>Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.</li> <li>Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.</li> <li>Automatycznie wykonywane rewizje konfiguracji.</li> </ul>	
5.	Parametry wydajnościowe	<ul style="list-style-type: none"> <li>Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps.</li> <li>Tablica adresów MAC o pojemności co najmniej 32k wpisów.</li> <li>Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.</li> </ul>	SPEŁNIA TAK /NIE
6.	Wymagane funkcje	<ul style="list-style-type: none"> <li>Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.</li> <li>Obsługa Jumbo Frames.</li> <li>Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).</li> <li>Agregacja portów zgodna ze standardem 802.3ad.</li> <li>Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.</li> <li>Obsługa routingu statycznego.</li> <li>Port-mirroring.</li> <li>Uwierzytelnianie 802.1x na poziomie portu.</li> <li>Uwierzytelnianie 802.1x w oparciu o adres MAC.</li> <li>W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).</li> <li>W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.</li> <li>W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.</li> <li>Obsługa protokołu sFlow.</li> </ul>	
7.	Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	<p>10. 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:</p> <ul style="list-style-type: none"> <li>Centralne zarządzanie konfiguracją urządzenia</li> </ul>	SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>• Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania</li> <li>• Centralne zarządzanie sieciami VLAN.</li> <li>• Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u</li> <li>• Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..</li> <li>• Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.</li> <li>• 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.</li> <li>• Automatyczna detekcja i rekomendacje konfiguracji.</li> <li>• Przesyłanie logów na zewnętrzny serwer syslog.</li> <li>• Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.</li> <li>• Obsługa białych i czarnych list adresów MAC.</li> <li>• Wykrywanie aplikacji komunikujących się w sieci.</li> </ul> <p>11. Musi być możliwe redundantne połączenie z elementami zarządzającymi.</p> <p>12. 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.</p>	
8.	Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	<ul style="list-style-type: none"> <li>• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.</li> <li>• System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.</li> </ul>	SPEŁNIA TAK /NIE
9.	Gwarancja oraz wsparcie	1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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.	SPEŁNIA TAK /NIE
10.	Rozszerzone wsparcie serwisowe	<p>7. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym Dniu Roboczym /w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy.</p> <p>8. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać <b>certyfiakat ISO 9001</b> w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku</p>	SPEŁNIA TAK /NIE

		<p>polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. Oferent winien przedłożyć dokumenty:</p> <ul style="list-style-type: none"> <li>• Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).</li> <li>• Certyfikat ISO 9001 podmiotu serwisującego.</li> </ul>	
14.	Opisy do wymagań ogólnych	<p>1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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.</p> <p>2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań</p>	SPEŁNIA TAK /NIE

## 8. PRZEŁĄCZNIK TYP V – SZT. 2

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1.	Charakterystyka ogólna	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych	<b>Producent</b>  <b>Model i wersja</b>
2.	Parametry fizyczne platformy	<ul style="list-style-type: none"> <li>• Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.</li> <li>• Zasilanie AC 230V.</li> <li>• Maksymalny pobór mocy: 60 W.</li> <li>• Minimalny zakres temperatury pracy: 0-40°C.</li> </ul>	SPEŁNIA TAK /NIE
3.	Interfejsy sieciowe - wymagania minimalne	<p>1. Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:</p> <p>a) 48 porty GE RJ-45.</p> <p>b) 4 porty 10 GE SFP+.</p>	SPEŁNIA TAK /NIE
4.	Zarządzanie	<ul style="list-style-type: none"> <li>• Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).</li> <li>• Wsparcie dla SNMP w wersjach 1-3</li> </ul>	SPEŁNIA TAK /NIE

## na Rozwój Cyfrowy

		<ul style="list-style-type: none"> <li>Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.</li> <li>Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.</li> <li>Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.</li> <li>Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).</li> <li>Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.</li> <li>Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.</li> <li>Automatycznie wykonywane rewizje konfiguracji.</li> </ul>	
5.	Parametry wydajnościowe	<ul style="list-style-type: none"> <li>Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.</li> <li>Tablica adresów MAC o pojemności co najmniej 32k wpisów.</li> <li>Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.</li> </ul>	SPEŁNIA TAK /NIE
6.	Wymagane funkcje	<ul style="list-style-type: none"> <li>Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.</li> <li>Obsługa Jumbo Frames.</li> <li>Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).</li> <li>Agregacja portów zgodna ze standardem 802.3ad.</li> <li>Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.</li> <li>Obsługa routingu statycznego.</li> <li>Port-mirroring.</li> <li>Uwierzytelnianie 802.1x na poziomie portu.</li> <li>Uwierzytelnianie 802.1x w oparciu o adres MAC.</li> <li>W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).</li> <li>W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.</li> <li>W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.</li> <li>Obsługa protokołu sFlow.</li> </ul>	
7.	Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	<p>13. 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:</p> <ul style="list-style-type: none"> <li>Centralne zarządzanie konfiguracją urządzenia</li> <li>Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania</li> <li>Centralne zarządzanie sieciami VLAN.</li> <li>Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u</li> <li>Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..</li> </ul>	SPEŁNIA TAK /NIE

## na Rozwój Cyfrowy

		<ul style="list-style-type: none"> <li>• Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.</li> <li>• 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.</li> <li>• Automatyczna detekcja i rekomendacje konfiguracji.</li> <li>• Przesyłanie logów na zewnętrzny serwer syslog.</li> <li>• Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.</li> <li>• Obsługa białych i czarnych list adresów MAC.</li> <li>• Wykrywanie aplikacji komunikujących się w sieci.</li> </ul> <p>14. Musi być możliwe redundantne połączenie z elementami zarządzającymi.</p> <p>15. 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.</p>	
8.	Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	<ul style="list-style-type: none"> <li>• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.</li> <li>• System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.</li> </ul>	SPEŁNIA TAK /NIE
9.	Gwarancja oraz wsparcie	1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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.	SPEŁNIA TAK /NIE
10.	Rozszerzone wsparcie serwisowe	<p>9. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym Dniu Roboczym /w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy.</p> <p>10. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać <b>certyfikat ISO 9001</b> w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. Oferent winien przedłożyć dokumenty:</p> <ul style="list-style-type: none"> <li>• Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).</li> <li>• Certyfikat ISO 9001 podmiotu serwisującego.</li> </ul>	SPEŁNIA TAK /NIE

## na Rozwój Cyfrowy

15.	Opisy do wymagań ogólnych	<p>1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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.</p> <p>2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań</p>	SPEŁNIA TAK /NIE
-----	---------------------------	---	------------------

## 9. FIREWALL SPRZĘTOWY – 1 SZT.

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
-----	----------	---------------------------------------	---------------------

## na Rozwój Cyfrowy

1.	<b>Wymagania Ogólne</b>	<p>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.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> <li>• Firewall.</li> <li>• Ochrony w warstwie aplikacji.</li> <li>• Protokołów routingu dynamicznego.</li> </ul>	<p><b>Producent</b></p> <p><b>Nazwa i wersja</b></p> <p>SPEŁNIA TAK /NIE</p>
2.	Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"> <li>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.</li> <li>2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</li> <li>3. Monitoring stanu realizowanych połączeń VPN.</li> <li>4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.</li> </ol>	SPEŁNIA TAK /NIE
3.	Interfejsy, Dysk, Zasilanie	<ol style="list-style-type: none"> <li>1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: <ul style="list-style-type: none"> <li>• 16 portami Gigabit Ethernet RJ-45.</li> <li>• 8 gniazdami SFP 1 Gbps.</li> <li>• 2 gniazdami SFP+ 10 Gbps.</li> </ul> </li> <li>2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</li> <li>3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.</li> <li>4. System jest wyposażony w zasilanie AC.</li> </ol>	SPEŁNIA TAK /NIE

## na Rozwój Cyfrowy

4.	Parametry wydajnościowe	<ol style="list-style-type: none"> <li>1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.</li> <li>2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.</li> <li>3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.</li> <li>4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps.</li> <li>5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.</li> <li>6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.</li> <li>7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.</li> </ol>	SPEŁNIA TAK /NIE
5.	Funkcje Systemu Bezpieczeństwa	<p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none"> <li>1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.</li> <li>2. Kontrola Aplikacji.</li> <li>3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.</li> <li>4. Ochrona przed malware.</li> <li>5. Ochrona przed atakami - Intrusion Prevention System.</li> <li>6. Kontrola stron WWW.</li> <li>7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.</li> <li>8. Zarządzanie pasmem (QoS, Traffic shaping).</li> <li>9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).</li> <li>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.</li> <li>11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.</li> <li>12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.</li> <li>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)</li> </ol>	SPEŁNIA TAK /NIE

6.	Polityki, Firewall	<ol style="list-style-type: none"> <li>1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</li> <li>2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: <ul style="list-style-type: none"> <li>• Translację jeden do jeden oraz jeden do wielu.</li> <li>• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.</li> </ul> </li> <li>3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</li> <li>4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.</li> <li>5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</li> <li>6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</li> <li>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. <ul style="list-style-type: none"> <li>• Amazon Web Services (AWS).</li> <li>• Microsoft Azure.</li> <li>• Cisco ACI.</li> <li>• Google Cloud Platform (GCP).</li> <li>• OpenStack.</li> <li>• VMware NSX.</li> <li>• Kubernetes.</li> </ul> </li> </ol>	SPEŁNIA TAK /NIE
7.	Połączenia VPN	<ol style="list-style-type: none"> <li>1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: <ul style="list-style-type: none"> <li>• Wsparcie dla IKE v1 oraz v2.</li> <li>• Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).</li> <li>• Obsługę protokołu Diffie-Hellman grup 19, 20.</li> <li>• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.</li> <li>• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.</li> <li>• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</li> <li>• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.</li> <li>• Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.</li> <li>• Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.</li> </ul> </li> </ol>	SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.</li> <li>Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.</li> <li>Mechanizm „Split tunneling” dla połączeń Client-to-Site.</li> </ul> <p>2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> <li>Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.</li> <li>Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.</li> </ul> <p>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</p>	
8.	Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <ol style="list-style-type: none"> <li>1. Routingu statycznego.</li> <li>2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).</li> <li>3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.</li> <li>4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.</li> <li>5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.</li> <li>6. BFD (Bidirectional Forwarding Detection).</li> <li>7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.</li> </ol>	SPEŁNIA TAK /NIE
9.	Funkcje SD-WAN	<ol style="list-style-type: none"> <li>1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</li> <li>2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</li> </ol>	SPEŁNIA TAK /NIE
10.	Zarządzanie pasmem	<ol style="list-style-type: none"> <li>1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</li> <li>2. System daje możliwość określania pasma dla poszczególnych aplikacji.</li> <li>3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</li> <li>4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.</li> </ol>	SPEŁNIA TAK /NIE

## na Rozwój Cyfrowy

11.	Ochrona przed malware	<ol style="list-style-type: none"> <li>1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</li> <li>2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</li> <li>3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.</li> <li>4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</li> <li>5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</li> <li>6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</li> <li>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 chmurze.</li> <li>8. System wstrzymuje dostarczenie pliku, dla którego jest realizowana analiza z wykorzystaniem systemu Sandbox, do czasu otrzymania werdyktu z systemu Sandbox.</li> <li>9. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.</li> <li>10. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</li> <li>11. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</li> </ol>	SPEŁNIA TAK /NIE
12.	Ochrona przed atakami	<p>Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>System chroni przed atakami na aplikacje pracujące na niestandardowych portach.</p> <p>Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p> <p>Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</p>	SPEŁNIA TAK /NIE

		<p>Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.</p> <p>Wykrywanie i blokowanie komunikacji C&amp;C do sieci botnet.</p> <p>Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy</p>	
13.	Kontrola aplikacji	<p>Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p> <p>Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</p> <p>Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>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).</p>	SPEŁNIA TAK /NIE
14.	Kontrola WWW	<p>Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p> <p>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.</p> <p>Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.</p> <p>Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</p> <p>Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</p> <p>Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</p>	SPEŁNIA TAK /NIE

		<p>Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</p> <p>System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji</p>	
15.	Uwierzytelnianie użytkowników w ramach sesji	<p>System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:</p> <p>Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</p> <p>Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</p> <p>Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</p> <p>System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</p> <p>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.</p> <p>Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p>	SPEŁNIA TAK /NIE
16.	Zarządzanie	<p>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.</p> <p>Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>Istnieje możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.</p> <p>System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</p> <p>System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p>	SPEŁNIA TAK /NIE

		<p>Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</p> <p>Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</p> <p>Logowanie</p> <p>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.</p> <p>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.</p> <p>Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>Możliwość włączenia logowania per reguła w polityce firewall.</p> <p>System zapewnia możliwość logowania do serwera SYSLOG.</p> <p>Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p> <p>Testy wydajnościowe oraz funkcjonalne</p> <p>Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.</p>	
17.	Serwisy i licencje	<p>Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:</p> <p>a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.</p> <p>Gwarancja oraz wsparcie</p> <p>System jest objęty serwisem gwarancyjnym producenta przez okres [12] miesiące polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie zamawiającego, realizowana przez producenta lub autoryzowanego dystrybutora w języku polskim przez okres wymaganej gwarancji.</p>	

		<p>Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji.</p> <p>Do zamawianego sprzętu Wykonawca zapewni usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:</p> <p>obsługa procesu RMA u producenta,</p> <p>zdalna pomoc w skonfigurowaniu urządzenia do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producenta,</p> <p>jednorazowa podstawowa konfiguracja platformy realizowana przez inżyniera z najwyższym dostępnym poziomem certyfikacji technicznej producenta,</p> <p>dostęp do szkolenia wideo prezentującego najlepsze praktyki współpracy z suportem producenta systemu realizującego funkcję Firewall.</p> <p>Dostęp do usługi powinien być świadczony przez dedykowaną infolinię (należy podać numer telefonu) oraz przez dedykowany moduł internetowy (należy podać adres).</p> <p>Usługa ta ma być świadczona przez podmiot posiadający certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.</p> <p>Do oferty należy załączyć oświadczenie producenta lub Autoryzowanego Dystrybutora o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001 oraz certyfikat potwierdzający posiadany najwyższy poziom certyfikacji technicznej producenta .</p>	
18.	Rozszerzone wsparcie serwisowe AHB/SOS	<p>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 36 miesięcy 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</p> <p>System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:</p> <p>Wsparcie telefoniczne zespołu certyfikowanych inżynierów.</p> <p>Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.</p>	<p><b>Producent</b></p> <p>Nazwa i wersja usługi</p>

		<p>Doradztwo w zakresie konfiguracji.</p> <p>Zdalne wsparcie techniczne.</p> <p>Pomoc w zakładaniu zgłoszeń serwisowych u producenta.</p> <p>Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).</p> <p>Przygotowanie urządzenia do zdalnej konfiguracji.</p> <p>Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.</p> <p>Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.</p> <p>Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.</p> <p>Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.</p> <p>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. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.</p> <p>Wymagania powinny być potwierdzone dokumentami: Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).</p> <p>Certyfikat ISO 9001 podmiotu serwisującego. Załączyć do oferty</p>	
<b>TESTY PENETRACYJNE INFRASTRUKTURY INFORMATYCZNEJ</b>			
1.	Informacje ogólne	<ul style="list-style-type: none"> <li>Głównym celem testów bezpieczeństwa jest identyfikacja możliwie wielu luk w zabezpieczeniach w szczególności tych, które mogą mieć poważny wpływ na atrybuty bezpieczeństwa systemów i danych przetwarzanych przez systemy (poufność, integralność, dostępność).</li> <li>Prace zostaną przeprowadzone zdalnie z wykorzystaniem połączenia VPN do zasobów Zamawiającego.</li> <li>Prace będą wykonywane z jednego stałego adresu IP Wykonawcy.</li> <li>Testy bezpieczeństwa muszą objąć wymagania weryfikacyjne określone w następujących dokumentach: <ul style="list-style-type: none"> <li>OWASP Web Security Testing Guide v4.2,</li> </ul> </li> </ul>	SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>OWASP Top 10 2021,</li> <li>OWASP Application Security Verification Standard (ASVS) v4.0.3 (Level 2),</li> </ul> <p>Przebieg procesu testowania bezpieczeństwa aplikacji</p>	
2.	Testy penetracyjne infrastruktury wewnętrznej	<ul style="list-style-type: none"> <li>Próby zgromadzenia jak największej ilości dostępnych publicznie informacji na temat infrastruktury informatycznej</li> <li>Identyfikacja udostępnionych usług poprzez skanowanie portów TCP/UDP wraz z próbą uzyskania informacji o zainstalowanych wersjach oprogramowania wykorzystując techniki fingerprinting oraz banner grabbing</li> <li>Skanowanie podatności z wykorzystaniem automatycznych narzędzi</li> <li>Manualna identyfikacja podatności</li> <li>w oparciu o zgromadzone informacje</li> <li>o wersjach zainstalowanego na badanych urządzeniach oprogramowania w publicznych bazach (np. Bugtraq, CERT, OSVDB),</li> <li>Analiza mająca na celu weryfikację i eliminację potencjalnych fałszywych alarmów (false positives) oraz identyfikację krytycznych podatności,</li> <li>Próba odnalezienia kodu oprogramowania wykorzystującego daną podatność – tzw. exploit</li> <li>Kontrolowane próby wykorzystania stwierdzonych podatności</li> </ul> <p>Testy podatności są realizowane w oparciu o globalną metodykę, zgodną z opracowaniami OSSTMM (Open Source Security Testing Methodology Manual) LPT (License Penetration Testing) oraz najlepszymi praktykami w obszarze testów podatności.</p> <ul style="list-style-type: none"> <li>Testy penetracyjne infrastruktury prowadzone będą z wykorzystaniem automatycznych narzędzi służących do weryfikacji poziomu bezpieczeństwa infrastruktury oraz przy wykorzystaniu technik manualnych,</li> <li>Minimalne narzędzia jakie Wykonawca musi wykorzystać do przeprowadzenia testów zewnętrznych:             <ul style="list-style-type: none"> <li>Nmap</li> <li>Nessus Professional</li> <li>OpenVAS</li> <li>MetaSploit</li> <li>Foca</li> <li>Maltego</li> <li>Skrypty i narzędzia autorskie w Kali linux,</li> </ul> </li> </ul> <p>Skrypty i narzędzia autorskie powershell do enumeracji infrastruktury Microsoft Windows,</p>	SPEŁNIA TAK /NIE

3.		<ul style="list-style-type: none"> <li>Zamawiający wymaga, aby Wykonawca posiada potencjał osobowy niezbędny do wykonania zamówienia. Zamawiający wymaga aby osoby testujące łącznie posiadały poniższe certyfikaty: <ul style="list-style-type: none"> <li>Offensive Security Certified Professional (OSCP);</li> <li>Certified Information Systems Security Professional (CISSP);</li> <li>Certified Security Analyst (ECSA);</li> <li>Web Application Penetration Tester (eWPT);</li> <li>Certified Professional Penetration Tester (eCPPT);</li> </ul> </li> </ul> <p>Certyfikaty należy załączyć do oferty</p>	SPEŁNIA TAK /NIE
----	--	---	------------------

## 10. NAS TYP I – 1 SZT.

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
3.	<b>Przeznaczenie</b>	<p>Wdrożenie rozwiązania NAS ma na celu stworzenie odseparowanego środowiska do przechowywania i testowania zarchiwizowanych danych. System ten zapewnia bezpieczne przechowywanie, zarządzanie oraz dostęp do danych w sposób wydajny i skalowalny. Dodatkowo, wdrożenie systemu wersjonowania plików umożliwi śledzenie i odzyskiwanie wcześniejszych wersji, co jest kluczowe w procesach testowania i archiwizacji. Dzięki temu możliwe będzie szybkie identyfikowanie i przywracanie wcześniejszych wersji plików, co zwiększy integralność danych oraz ułatwi zarządzanie zmianami w środowisku testowym.</p> <p>Dostarczone urządzenie a pełnić będzie również rolę urządzenia brzegowego do zarządzania tożsamością oraz dostęпами użytkowników dla maksymalizacji bezpieczeństwa organizacji dostępu do danych w siedzibie Zamawiającego</p>	<p><b>Producent</b></p> <p><b>Model /wersja</b></p>
4.	<b>Obudowa</b>	Typu rack o wysokości maksymalnie 2U wraz z szynami przesuwными umożliwiającymi montaż w szafie rack w zestawie. Obudowa musi zawierać minimum 2 kontrolery pracujące w układzie nadmiarowym typu active-passive.	SPEŁNIA TAK /NIE
5.	<b>Procesor</b>	Jeden procesor osiągający wynik minimum 9800 punktów w teście PassMark na każdy kontroler.	SPEŁNIA TAK /NIE
6.	<b>Pamięć RAM</b>	Minimum 64GB DDR4 ECC w konfiguracji 4 x 16GB na każdy kontroler. Model pamięci musi znajdować się na oficjalnej liście zgodności producenta – nie zezwala się na stosowanie zamienników.	SPEŁNIA TAK /NIE
7.	<b>Ilość obsługiwanych dysków</b>	Minimum 12 dysków o maksymalnej pojemności nie mniejszej niż 20 TB każdy, po podłączeniu modułów rozszerzających minimum 36 dysków.	
8.	<b>Interfejsy sieciowe</b>	Minimum 2 porty 1GbE RJ-45 na kontroler. Minimum 1 port 10GbE RJ-45 na kontroler.	SPEŁNIA TAK /NIE

		Minimum 2 porty 10GbE SFP+ na kontroler. Wsparcie dla agregacji łączy..	
9.	<b>Wskaźniki LED</b>	Status, HDD 1-12, zasilanie	SPEŁNIA TAK /NIE
10.	<b>Obsługa RAID</b>	RAID 0, 1, 5, 6, 10 wraz z obsługą dysków typu hot spare.	SPEŁNIA TAK /NIE
11.	<b>Funkcje RAID</b>	Możliwość zwiększania pojemności i migracja między poziomami RAID online.	SPEŁNIA TAK /NIE
12.	<b>Szyfrowanie</b>	Możliwość szyfrowania wybranych udziałów sieciowych.	SPEŁNIA TAK /NIE
13.	<b>Protokoły</b>	SMB, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP, VPN (OpenVPN™, L2TP)	SPEŁNIA TAK /NIE
14.	<b>Usługi</b>	<p>1. Serwer VPN, Serwer pocztowy dla kilku domen, Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antywirus, Usługa DDNS, 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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• Obsługa wszystkich typów i wersji sprzętu wirtualnego VMware, w tym 62TB VMDK.</li> <li>• 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.</li> <li>• 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.</li> <li>• Kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym konfiguracji danych i systemu.</li> <li>• Kopia zapasowa bez agentów.</li> <li>• Korzystanie z funkcji VMware Changed Block Tracking i funkcji Hyper-V Resilient Change Tracking do wykonywania przyrostowej kopii zapasowej</li> <li>• Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowych.</li> <li>• 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.</li> <li>• 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.</li> <li>• Kopia zapasowa uwzględniająca aplikacje dla maszyn wirtualnych VMware vSphere lub Microsoft Hyper-V działających w systemie</li> </ul>	SPEŁNIA TAK /NIE

## na Rozwój Cyfrowy

		<p>Microsoft Windows 2003 SP1 lub nowszym (z wyjątkiem Nano Server z powodu braku architektury VSS).</p> <ul style="list-style-type: none"> <li>Obsługa tworzenia kopii zapasowych systemów operacyjnych i aplikacji obsługiwanych przez rozwiązania VMware vSphere i Microsoft Hyper-V.</li> </ul> <p>3. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 7 lub nowszym według harmonogramu z możliwością zarządzania z poziomu centralnej konsoli dostępnej lokalnie oraz zdalnie, przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Dane z kopii zapasowych muszą być redukowane poprzez globalną deduplikację po stronie miejsca przechowywania. Licencja musi umożliwiać podłączanie kolejnych komputerów do systemu kopii zapasowej bez limitu.</p>	
15.	<b>Obsługa migawek</b>	Liczba migawek folderu współdzielonego: minimum 1000	SPEŁNIA TAK /NIE
16.	<b>Zarządzanie dyskami</b>	SMART, sprawdzanie złych sektorów.	SPEŁNIA TAK /NIE
17.	<b>Język GUI</b>	Polski	SPEŁNIA TAK /NIE
18.	<b>Gwarancja i serwis</b>	Minimum 36 miesięcy gwarancji Next Business Day producenta na serwer.	SPEŁNIA TAK /NIE
19.	<b>Waga bez dysków</b>	Maksymalnie 25 kg	SPEŁNIA TAK /NIE
20.	<b>Pobór mocy</b>	Maksymalnie 500W w trybie pracy.	SPEŁNIA TAK /NIE
21.	<b>Certyfikaty</b>	CE, FCC	SPEŁNIA TAK /NIE
22.	<b>System plików</b>	Dyski wewnętrzne: BTRFS.	SPEŁNIA TAK /NIE
23.	<b>Szyfrowanie</b>	Mechanizm szyfrowania sprzętowego (AES-NI)	SPEŁNIA TAK /NIE
24.	<b>Liczba wolumenów</b>	Minimum 60	SPEŁNIA TAK /NIE
25.	<b>Liczba iSCSI Targetów</b>	Minimum 250	SPEŁNIA TAK /NIE
26.	<b>Liczba iSCSI LUN</b>	Minimum 250	SPEŁNIA TAK /NIE
27.	<b>Liczba kont lokalnych użytkowników</b>	Minimum 10000	SPEŁNIA TAK /NIE
28.	<b>Liczba grup</b>	Minimum 500	SPEŁNIA TAK /NIE
29.	<b>Liczba folderów udostępnionych</b>	Minimum 500	SPEŁNIA TAK /NIE
30.	<b>Zasilacz</b>	Redundantny zasilacz o mocy minimalnej 500W.	SPEŁNIA TAK /NIE
31.	<b>Chłodzenie</b>	Minimum 2 wentylatory z możliwością regulowania prędkości obrotowej oraz wymiany w urządzeniu podczas pracy.	SPEŁNIA TAK /NIE
32.	<b>Gwarancja</b>	Minimum 36 miesięcy gwarancji Next Business Day On-site producenta – gwarantowany termin naprawy sprzętu przez dedykowanego inżyniera w przypadku awarii sprzętowej na następny dzień roboczy z opcją pozostawienia uszkodzonego nośnika u Zgłaszającego.	<p><b>Producent</b></p> <p><b>PN pakietu identyfikujący oferowany serwis</b></p> <p>SPEŁNIA TAK /NIE</p>
33.	<b>Dodatkowe Wsparcie techniczne</b>	<p><b>Zakres dodatkowego wsparcia</b></p> <p>Wsparcie techniczne musi być świadczone przez wykwalifikowanych inżynierów Producenta oferowanego</p>	

		<p>rozwiązania lub certyfikowanych inżynierów dystrybutora oferowanego rozwiązania na terenie Polski posiadającego autoryzację producenta od minimum 10 lat. Wymagane jest, aby osoby te posiadały odpowiednie kompetencje techniczne i doświadczenie w obsłudze oraz serwisowaniu urządzeń objętych niniejszą dostawą, co zapewni najwyższy poziom jakości usług oraz bezpieczeństwo danych Zamawiającego.</p> <ol style="list-style-type: none"> <li><b>Proaktywne monitorowanie infrastruktury</b> <ul style="list-style-type: none"> <li>○ Ciągłe monitorowanie pracy urządzeń, obejmujące: <ul style="list-style-type: none"> <li>▪ Stan techniczny nośników danych, w tym parametry SMART, zużycie i temperaturę.</li> <li>▪ Wykorzystanie zasobów systemowych, takich jak procesor, pamięć i przestrzeń dyskowa.</li> <li>▪ Analizę logów systemowych pod kątem potencjalnych zagrożeń i anomalii.</li> </ul> </li> <li>○ Automatyczne powiadomienia o wykrytych problemach technicznych przesyłane do administratora Zamawiającego oraz zespołu wsparcia.</li> </ul> </li> <li><b>Kwartalne raportowanie stanu infrastruktury</b> <ul style="list-style-type: none"> <li>○ Przygotowywanie szczegółowych raportów technicznych zawierających: <ul style="list-style-type: none"> <li>▪ Stan urządzeń, w tym status macierzy dyskowych oraz aktualną konfigurację systemową.</li> <li>▪ Wykorzystanie zasobów i ich dynamikę w okresie sprawozdawczym.</li> <li>▪ Informacje o liczbie zgłoszeń serwisowych, podejmowanych działaniach oraz ich wynikach.</li> <li>▪ Rekomendacje dotyczące optymalizacji wydajności i planowania przyszłych działań.</li> </ul> </li> <li>○ Raporty dostarczane w formie elektronicznej oraz omawiane podczas cyklicznych spotkań technicznych z przedstawicielami Zamawiającego.</li> </ul> </li> <li><b>Reakcja serwisowa i wsparcie w sytuacjach krytycznych</b> <ul style="list-style-type: none"> <li>○ Gwarantowany czas reakcji na zgłoszenia: <ul style="list-style-type: none"> <li>▪ Krytyczne awarie: <b>maksymalnie 1 godzina</b> od zgłoszenia.</li> <li>▪ Problemy o wysokim priorytecie: <b>do 4 godzin roboczych</b>.</li> <li>▪ Problemy o niskim priorytecie: <b>do 1 dnia roboczego</b>.</li> </ul> </li> </ul> </li> <li><b>Przeglądy techniczne i diagnostyka</b></li> </ol>	SPEŁNIA TAK/NIE
--	--	---	-----------------

- Realizacja kwartalnych przeglądów technicznych obejmujących:
  - Weryfikację stanu nośników danych i macierzy RAID.
  - Aktualizację systemów operacyjnych oraz aplikacji zainstalowanych na urządzeniach.
  - Testowanie procedur odzyskiwania danych z kopii zapasowych.
  - Sprawdzanie konfiguracji systemów zabezpieczeń oraz logów w celu identyfikacji potencjalnych zagrożeń.
- Każdy przegląd kończy się sporządzeniem szczegółowego raportu dla Zamawiającego wraz z rekomendacjami.

#### 5. Analiza ryzyk i doradztwo techniczne

- Regularne identyfikowanie potencjalnych zagrożeń dla działania urządzeń oraz opracowanie planów zapobiegawczych.
- Bieżąca analiza wydajności oraz analiza ryzyk związanych z przetwarzaniem danych.
- Proponowanie działań optymalizacyjnych, dostosowanych do zmieniających się potrzeb Zamawiającego.

#### 6. Wsparcie w integracji i optymalizacji infrastruktury

- Pomoc techniczna przy integracji urządzeń z istniejącą infrastrukturą sieciową i systemami informatycznymi Zamawiającego.
- Konfiguracja i utrzymanie mechanizmów zabezpieczeń danych, w tym systemów tworzenia kopii zapasowych oraz ich odtwarzania.

Dostosowanie konfiguracji urządzeń do zmieniających się wymagań operacyjnych, zapewniające optymalne wykorzystanie zasobów

#### Oferent winien przedłożyć dokumenty:

Dokument potwierdzony przez Producenta lub Autoryzowanego Dystrybutora producenta o gotowości świadczenia na rzecz Zamawiającego wymaganego wsparcia (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).

## 11. DYSKI DO NAS TYP I – 12 SZT.

L.P	Parametr	Charakterystyka (wymagania minimalne)	
	<b>Zainstalowane dyski</b>	<p>12 dysków o pojemności 12 TB każdy zgodnych z listą kompatybilności oferowanego rozwiązania oraz charakteryzujących się następującymi parametrami:</p> <ul style="list-style-type: none"> <li>- prędkość obrotowa: minimum 7200 RPM,</li> <li>- pamięć cache: minimum 250 MB,</li> <li>- gwarancja: minimum 36 miesięcy,</li> <li>- MTBF: minimum 2,5 miliona.</li> </ul> <p>W przypadku awarii dysku twardego uszkodzony nośnik pozostaje własnością Zamawiającego.</p>	<p><b>Producent</b></p> <p><b>Model</b></p> <p><b>ilość</b></p> <p>SPEŁNIA TAK /NIE</p>

## 12. NAS TYP II – 1 SZT.

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1.	<b>Przeznaczenie</b>	<p>Bezpieczne przechowywanie danych – system NAS zapewni bezpieczne składowanie logów zebranych przez dedykowane oprogramowanie, chroniąc przed utratą lub uszkodzeniem danych.</p> <p>Centralizacja logów – NAS umożliwi centralne przechowywanie i zarządzanie logami z różnych źródeł, co ułatwi ich dostęp i analizę.</p> <p>Skalowalność – system NAS pozwala na elastyczne zwiększanie pojemności w miarę rosnących potrzeb w zakresie przechowywania logów.</p> <p>Szybki dostęp do danych – zapewnia szybki odczyt i zapis danych, co jest kluczowe w przypadku intensywnej analizy logów.</p> <p>Redundancja i kopie zapasowe – dzięki systemom RAID i możliwości tworzenia kopii zapasowych, NAS zwiększa odporność na awarie.</p>	<p><b>Producent</b></p> <p><b>Model /wersja</b></p> <p>SPEŁNIA TAK /NIE</p>
2.	<b>Procesor</b>	Jeden procesor osiągający wynik minimum 4000 punktów w teście PassMark.	SPEŁNIA TAK /NIE
3.	<b>Obudowa</b>	Typu rack o wysokości maksymalnej 1U z szynami przesuwными do instalacji w szafie rack w zestawie.	SPEŁNIA TAK /NIE
4.	<b>Pamięć RAM</b>	Minimum 32GB DDR4 ECC tego samego producenta co serwer.	SPEŁNIA TAK /NIE
5.	<b>Interfejsy sieciowe</b>	<p>Minimum 4 porty 1GbE RJ-45.</p> <p>Minimum 1 port 10GbE RJ-45</p> <p>Minimum 1 port 10GbE SFP</p> <p>Obsługa agregacji łączy.</p>	SPEŁNIA TAK /NIE

6.	<b>Ilość obsługiwanych dysków</b>	Minimum 4 dyski o maksymalnej pojemności nie mniejszej niż 18TB każdy, po podłączeniu modułów rozszerzających minimum 8 dysków.	SPEŁNIA TAK /NIE
7.	<b>Zainstalowane dyski</b>	<p>4 dyski o pojemności 12 TB każdy zgodne z listą kompatybilności oferowanego serwera NAS oraz charakteryzujące się następującymi parametrami:</p> <ul style="list-style-type: none"> <li>- prędkość obrotowa: minimum 7200 RPM,</li> <li>- pamięć cache: minimum 256 MB,</li> <li>- MTBF: minimum 2miliony,</li> <li>- gwarancja: minimum 36 miesięcy,</li> <li>- możliwość aktualizowania oprogramowania dysków w czasie rzeczywistym podczas pracy serwera.</li> </ul> <p>W przypadku awarii dysku twardego uszkodzony nośnik pozostaje własnością Zamawiającego.</p>	<p><b>Producent</b></p> <p><b>Model</b></p> <p>SPEŁNIA TAK /NIE</p>
8.	<b>Gniazda rozszerzeń</b>	1 slot PCIe 3.0 x8 (x4 link)	SPEŁNIA TAK /NIE
9.	<b>Wskaźniki LED</b>	Zasilanie, alert, status, LAN, HDD 1-4	SPEŁNIA TAK /NIE
10.	<b>Obsługa RAID</b>	Pojedynczy, JBOD, RAID 0, 1, 5, 6, 10, SHR wraz z obsługą dysków typu hot spare.	SPEŁNIA TAK /NIE
11.	<b>Funkcje RAID</b>	Możliwość zwiększania pojemności i migracja między poziomami RAID online.	SPEŁNIA TAK /NIE
12.	<b>Szyfrowanie</b>	Możliwość szyfrowania wybranych udziałów sieciowych.	SPEŁNIA TAK /NIE
13.	<b>Protokoły</b>	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP	SPEŁNIA TAK /NIE
14.	<b>Usługi</b>	<p>1. Serwer VPN, Serwer pocztowy dla kilku domen, Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antyvirus, Usługa DDNS, 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.</p> <p>2. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 7 lub nowszym według harmonogramu z centralnej konsoli zarządzania dostępnej lokalnie oraz zdalnie, z możliwością przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem</p>	SPEŁNIA TAK /NIE

		<p>w sposób automatyczny poprzez dedykowany algorytm. Bez ograniczenia liczby podłączanych komputerów do systemu kopii zapasowej.</p> <p>3. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klastr obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora.</p>	
15.	<b>Zarządzanie dyskami</b>	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów,	SPEŁNIA TAK /NIE
16.	<b>Język GUI</b>	Polski	SPEŁNIA TAK /NIE
17.	<b>Gwarancja i serwis</b>	Minimum 36 miesięcy gwarancji Next Business Day producenta <u>na serwer oraz dyski HDD.</u>	SPEŁNIA TAK /NIE
18.	<b>Pobór mocy</b>	Maksymalnie 55W w trybie pracy.	SPEŁNIA TAK /NIE
19.	<b>Certyfikaty</b>	FCC, CE	SPEŁNIA TAK /NIE
20.	<b>System plików</b>	Dyski wewnętrzne: BTRFS. Dyski zewnętrzne: FAT, NTFS, EXT3, EXT4, HFS+.	SPEŁNIA TAK /NIE
21.	<b>Zasilanie</b>	Redundantny zasilacz o mocy minimum 150W	SPEŁNIA TAK /NIE
22.	<b>Gwarancja</b>	Pakiet serwisowy na okres minimum 36 miesięcy działający w trybie 5/13 NBD na cały system złożony z serwera, dysków i akcesoriów - dostawa sprzętu zastępczego na następny dzień roboczy po wystąpieniu awarii sprzętowej, obowiązuje od poniedziałku do piątku w dni robocze z opcją pozostawienia uszkodzonego nośnika u Zgłaszającego.	<p><b>Producent</b></p> <p><b>PN pakietu identyfikujący oferowany serwis</b></p> <p>SPEŁNIA TAK /NIE</p>

### 13. OPROGRAMOWANIE DO ARCHIWIZACJI LOGÓW

-1 LICENCJA URZĄD

-1 LICENCJA OPS

L.P.	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1	Cel wdrożenia	Oprogramowanie do archiwizacji logów ma na celu gromadzenie, przechowywanie i organizowanie logów systemowych w sposób bezpieczny i zgodny z przepisami. Rozwiązanie to pozwala na długoterminowe	<b>Producent</b>

		archiwizowanie danych, co ułatwia analizę incydentów oraz spełnia wymogi audytowe i regulacyjne. Dzięki funkcjom wyszukiwania i filtrowania, oprogramowanie umożliwia szybki dostęp do potrzebnych informacji, wspierając tym samym zarządzanie bezpieczeństwem. Wdrożenie tego rozwiązania pozwala organizacji monitorować i analizować działania w systemach IT, minimalizując ryzyko potencjalnych zagrożeń.	<b>Nazwa i wersja oprogramowania</b>
2	Charakterystyka rozwiązania	<ol style="list-style-type: none"> <li>1. Rozwiązanie musi odbierać wiadomości Syslog</li> <li>2. Rozwiązanie musi odbierać wiadomości Trap SNMP w wersji v1,v2, v3</li> <li>3. Rozwiązanie musi nasłuchiwać Windows Event Log</li> <li>4. Rozwiązanie musi posiadać graficzny interfejs użytkownika w przeglądarce internetowej</li> <li>5. Rozwiązanie musi mieć możliwość powiadamiania użytkowników drogą emailową na bazie otrzymanych zdarzeń</li> <li>6. Rozwiązanie musi mieć możliwość uruchamiania zewnętrznych skryptów</li> <li>7. Rozwiązanie musi mieć możliwość przesyłania dalej zebranych wiadomości do innych systemów w formatach Syslog oraz Trap SNMP w wersji v1, v2, v3</li> <li>8. Rozwiązanie musi mieć możliwość eksportu zdarzeń do formatu .csv</li> <li>9. Rozwiązanie powinno umożliwiać zarządzanie politykami retencji danych zdarzeń</li> <li>10. Rozwiązanie musi wspierać standard IPv4 i IPv6</li> <li>11. Rozwiązanie musi wspierać przesył danych na poziomie powyżej 2 000 000 zdarzeń na godzinę</li> <li>12. Rozwiązanie musi być licencjonowane w sposób nieograniczający ilości podłączonych urządzeń przysyłających informacje</li> <li>13. Rozwiązanie powinno integrować się ze Splunk</li> <li>14. Rozwiązanie powinno integrować się z rozwiązaniami typu SIEM</li> <li>15. Rozwiązanie musi mieć możliwość instalacji na systemach Microsoft Windows Server 2016, 2019, 2022 oraz Microsoft Windows 10, 11.</li> </ol>	SPEŁNIA TAK /NIE
3	Licencjonowanie	Licencja wieczysta na oprogramowanie , na okres minimum 12 m-cy	SPEŁNIA TAK /NIE
4	Usługi	Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, : - instalacja i konfiguracja rozwiązania na platformie Zamawiającego - szkolenie dla administratora rozwiązania - wsparcie w języku polskim w trybie 8x5 w dni robocze	SPEŁNIA TAK /NIE

#### 14. OPROGRAMOWANIE DO TWORZENIA KOPII ZAPASOWYCH NA POTRZEBY URZĘDU

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1.	Charakterystyka oprogramowania	<ul style="list-style-type: none"> <li>• <b>Możliwość backupu licencja na 100 komputerów 4 serwerów, 2 hostów wirtualizacji</b></li> <li>• Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania</li> </ul>	<b>Producent oprogramowania</b>  Nazwa i wersja

wykonywaniem kopii zapasowych z dysków komputerów klienckich

- Program serwerowy kompatybilny z systemami: Microsoft Windows XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology
- Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology
- Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików)
- Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)
- Automatyczny backup przy wyłączaniu komputera
- Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych \* i ?
- Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows)
- Backup baz danych i plików poczty w trybie online i offline
- Kopie rotacyjne (wersjonowanie)
- Zapis archiwów w otwartym formacie (ZIP 64-bit)
- Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi
- Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore)
- Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej
- Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych
- Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO
- Kompresja po stronie stacji roboczej
- Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP,
- Replikacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows)
- Centralne sterowanie całym Systemem z jednego miejsca
- Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników
- Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN
- Wysyłanie Alertów administracyjnych na e-mail
- Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych
- Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki
- Automatyczna aktualizacja oprogramowania na komputerach zdalnych

SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>• Bezterminowa licencja - licencja nie może być ograniczona czasowo</li> <li>• Interfejs, instrukcja i pomoc techniczna w języku polskim</li> <li>• Replikacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows)</li> <li>• Możliwość instalacji klienta przez GPO</li> <li>• Współpraca z systemami Systemami Zarządzania Informacją i Zdarzeniami Bezpieczeństwa (SIEM - Security Information and Event Management)</li> <li>• Możliwość zastosowania własnych certyfikatów SSL</li> <li>• Dwuosobowa kontrola administracyjna</li> </ul>	
--	--	--	--

## 15. OPROGRAMOWANIE DO TWORZENIA KOPII ZAPASOWYCH NA POTRZEBY OPS

L.P	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1.	Charakterystyka oprogramowania	<ul style="list-style-type: none"> <li>• Możliwość backupu licencja na 50 komputerów 2 serwerów, 1 host wirtualizacji</li> <li>• Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich</li> <li>• Program serwerowy kompatybilny z systemami: Microsoft Windows XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology</li> <li>• Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology</li> <li>• Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików)</li> <li>• Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)</li> <li>• Automatyczny backup przy wyłączaniu komputera</li> <li>• Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i ?</li> <li>• Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows)</li> <li>• Backup baz danych i plików poczty w trybie online i offline</li> <li>• Kopie rotacyjne (wersjonowanie)</li> <li>• Zapis archiwów w otwartym formacie (ZIP 64-bit)</li> </ul>	<p><b>Producent oprogramowania</b></p> <p>Nazwa i wersja</p> <p>SPEŁNIA TAK /NIE</p>

		<ul style="list-style-type: none"> <li>• Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi</li> <li>• Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore)</li> <li>• Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej</li> <li>• Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych</li> <li>• Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO</li> <li>• Kompresja po stronie stacji roboczej</li> <li>• Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP,</li> <li>• Replikacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows)</li> <li>• Centralne sterowanie całym Systemem z jednego miejsca</li> <li>• Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników</li> <li>• Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN</li> <li>• Wysyłanie Alertów administracyjnych na e-mail</li> <li>• Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych</li> <li>• Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki</li> <li>• Automatyczna aktualizacja oprogramowania na komputerach zdalnych</li> <li>• Bezterminowa licencja - licencja nie może być ograniczona czasowo</li> <li>• Interfejs, instrukcja i pomoc techniczna w języku polskim</li> <li>• Replikacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows)</li> <li>• Możliwość instalacji klienta przez GPO</li> <li>• Współpraca z systemami Systemami Zarządzania Informacją i Zdarzeniami Bezpieczeństwa (SIEM - Security Information and Event Management)</li> <li>• Możliwość zastosowania własnych certyfikatów SSL</li> <li>• Dwuosobowa kontrola administracyjna</li> </ul>	
--	--	--	--

## 16. DYSKI DO MACIERZY - 14 SZT

L.P.	Parametr	Charakterystyka (wymagania minimalne)	Oferowane parametry
1	Kompatybilność	Przedmiotem zamówienia jest dostawa 12 sztuk dysków SSD o pojemności 3.84 TB, w pełni kompatybilnych z macierzą <b>Dell ME5024</b> , posiadaną przez Zamawiającego. Zamawiający dopuszcza zaoferowanie dysków równoważnych, pod warunkiem, że będą spełniały wszystkie wymienione poniżej parametry techniczne oraz funkcjonalne. W przypadku zaoferowania dysków równoważnych, Wykonawca zobowiązany jest dostarczyć pisemne	<p><b>Producent</b></p> <p><b>Model</b></p>

		potwierdzenie kompatybilności z macierzą Dell ME5024, wydane przez producenta lub autoryzowanego przedstawiciela producenta.	
2	<b>Pojemność dysku</b>	Minimum 3.84 TB (terabajty).	SPEŁNIA TAK /NIE
3	<b>Rodzaj dysku</b>	SSD (Solid State Drive) – dyski półprzewodnikowe, przeznaczone do zastosowań korporacyjnych.	SPEŁNIA TAK /NIE
4	<b>Interfejs</b>	SAS (Serial Attached SCSI) z obsługą prędkości do 24 Gbps.	SPEŁNIA TAK /NIE
5	<b>Rozmiar fizyczny</b>	2.5 cala, przystosowane do montażu w kieszeniach typu hot-plug.	SPEŁNIA TAK /NIE
6	<b>Przystosowanie do obciążeń</b>	Dyski zoptymalizowane do zastosowań typu Read-Intensive (RI) z cyklem zapisu wynoszącym minimum 1 DDPD (Drive Writes Per Day).	SPEŁNIA TAK /NIE
7	<b>Typ sektora</b>	512e (512 emulated).	SPEŁNIA TAK /NIE
8	<b>Zarządzanie zasilaniem</b>	Dyski o niskim poborze mocy, dostosowane do pracy w środowisku serwerowym o wysokiej gęstości.	SPEŁNIA TAK /NIE
9	<b>Funkcje bezpieczeństwa</b>	Obsługa funkcji Instant Secure Erase (ISE), umożliwiającej certyfikowane usuwanie danych z dysków zgodnie z międzynarodowymi standardami bezpieczeństwa.	SPEŁNIA TAK /NIE
10	<b>Wydajność operacyjna</b>	Przystosowane do pracy ciągłej w środowisku korporacyjnym, zapewniające wysoką szybkość odczytu/zapisu oraz niski czas dostępu.	SPEŁNIA TAK /NIE
11	<b>Warunki gwarancji i dodatkowe wymagania</b>	Minimum 5 lat wsparcia serwisowego z możliwością wymiany dysku w przypadku awarii. W przypadku uszkodzenia dysku w ramach gwarancji, dane znajdujące się na dysku muszą zostać certyfikowanie usunięte zgodnie z międzynarodowymi standardami (np. NIST 800-88r1). Firma serwisująca i wykonująca usługę certyfikowanego usunięcia danych, musi posiadać ISO 27001 (Zarządzania Bezpieczeństwem Informacji (ISMS – Information Security Management System) – dokumenty należy załączyć do oferty. Ponadto, w przypadku zaoferowania równoważnych modeli dysków, Wykonawca musi dostarczyć dokumentację potwierdzającą kompatybilność z macierzą Dell ME5024.	SPEŁNIA TAK /NIE

## 17. WDROŻENIE

### OKABLOWANIE

#### 1. Okablowanie sieciowe i moduły SFP+

Wykonawca zobowiązany jest do dostarczenia pełnej ilości okablowania zapewniającego prawidłowe połączenie wszystkich dostarczonych urządzeń, w tym:

- przełączników sieciowych,
- serwerów,
- macierzy dyskowych,
- pozostałych elementów infrastruktury zgodnie z wymaganiami Zamawiającego.

#### 2. Minimalna wymagana ilość kabli i wkładek SFP+

Dla przełączników sieciowych (switchy):

- 5 szt. kabli 2m LC/UPC - SC/UPC
- 12 szt. kabli 1m LC/UPC - SC/UPC
- 4 szt. kabli 1m LC/UPC - LC/UPC
- 3 szt. kabli 8m LC/UPC - LC/UPC

## na Rozwój Cyfrowy

- 20 szt. wkładek jednomodowych SFP+ 10Gb
- 2 szt. wkładek wielomodowych lub jednomodowych SFP+ 10Gb wraz z 2 szt. kabli

1m

- LC np. BIDI SFP+ 1330nm 30KM SMP LC DDM

**Dla serwerów i macierzy dyskowych:**

- 12 szt. kabli 2m (SM/MM w zależności od wkładek)
- 1 szt. kabla SFP+ 10Gb o długości 5m
- 1 szt. kabla SFP+ 10Gb o długości 2m
- 12 szt. wkładek SFP+ 10Gb (dla serwerów i switchy)
- 2 szt. wkładek SFP+ 10Gb dla macierzy

**Uwagi :**

- Wykaz okablowania i modułów SFP+ przedstawiony powyżej należy traktować jako **minimalny wymagany zestaw**.
- **Wykonawca odpowiada za dostarczenie wszystkich brakujących kabli i połączeń**, które są niezbędne do zapewnienia pełnej funkcjonalności systemu, nawet jeśli nie zostały one wyraźnie wyszczególnione w zestawieniu.
- W przypadku stwierdzenia brakujących połączeń wykonawca jest zobowiązany do ich uzupełnienia **bez dodatkowych kosztów dla Zamawiającego**.

**3. Wymagania dotyczące instalacji i organizacji okablowania**

Wykonawca odpowiada za prawidłową instalację oraz organizację okablowania zgodnie z aktualnymi normami europejskimi:

- **EN 50173** – standard okablowania strukturalnego dla sieci teleinformatycznych
- **EN 50174** – wytyczne dotyczące instalacji i prowadzenia okablowania
- **EN 50310** – zasady ekranowania i uziemienia systemów telekomunikacyjnych
- **EN 50575** – klasyfikacja kabli w zakresie odporności ogniowej

**4. Dodatkowe wymagania dla instalacji:**

- Wszystkie kable muszą być prowadzone w sposób zgodny z wytycznymi norm **EN 50174-1, EN 50174-2 oraz EN 50174-3**.
- Instalacja musi uwzględniać odpowiednie promienie gięcia kabli, ich ekranowanie oraz separację od źródeł zakłóceń elektromagnetycznych (np. linii zasilających).
- Kable powinny być **oznakowane i ułożone w sposób umożliwiający łatwą identyfikację połączeń**.
- Organizacja i prowadzenie okablowania w szafach rackowych musi być zgodna z dobrą praktyką instalacyjną oraz uwzględniać **organizery kablów**.
- W przypadku stosowania kabli światłowodowych wykonawca musi zapewnić **odpowiednie zakończenia i ochronę** przed uszkodzeniami mechanicznymi.

**1. SERWER TYP I (2 szt.)**

Wdrożenie serwerów typu I obejmuje szereg działań mających na celu zapewnienie ich pełnej funkcjonalności jako kluczowych elementów infrastruktury IT, dedykowanych podniesieniu poziomu cyberbezpieczeństwa. W zakres wdrożenia wchodzi następujące etapy:

- **Dostawa i instalacja:** Dostarczone zostaną dwa serwery w obudowie Rack 2U, wyposażone w 12 wnęk na dyski 3,5", spełniające minimalne wymagania sprzętowe opisane w punktach 2-18 dokumentu. Serwery zostaną zainstalowane w wyznaczonym miejscu w infrastrukturze Zamawiającego.

SPEŁNIA TAK /NIE

<ul style="list-style-type: none"> <li>• <b>Konfiguracja sprzętowa:</b> Konfiguracja obejmuje m.in. instalację dysków twardych, kart sieciowych i innych niezbędnych komponentów, zapewnienie redundancji zasilania oraz konfigurację BIOS.</li> <li>• <b>Instalacja i konfiguracja systemu operacyjnego:</b> Zainstalowany zostanie system operacyjny Microsoft Windows Server 2019 lub 2022, wraz z niezbędnymi sterownikami i aktualizacjami.</li> <li>• <b>Instalacja i konfiguracja oprogramowania:</b> Na serwerach zainstalowane zostanie oprogramowanie dedykowane ochronie sieci i zarządzaniu bezpieczeństwem, w tym: <ul style="list-style-type: none"> <li>○ <b>Oprogramowanie do zarządzania serwerami:</b> Oprogramowanie to powinno spełniać wymagania opisane w punktach 19-21 dokumentu, umożliwiając m.in. zdalną administrację i monitorowanie, automatyczne zgłaszanie incydentów do centrum serwisowego producenta oraz tworzenie raportów o stanie i konfiguracji serwerów.</li> <li>○ <b>Oprogramowanie do monitorowania:</b> Oprogramowanie to, zgodne z wymaganiami punktów 20-21 dokumentu, powinno umożliwiać monitorowanie stanu i wydajności serwerów, wykrywanie anomalii i potencjalnych zagrożeń bezpieczeństwa oraz generowanie raportów i analiz.</li> <li>○ <b>Oprogramowanie antywirusowe:</b> Oprogramowanie antywirusowe będzie zarządzane z centralnej konsoli, a jego funkcjonalność musi spełniać wymagania opisane w punktach 26-43 dokumentu.</li> <li>○ <b>Oprogramowanie EDR (Endpoint Detection and Response):</b> Oprogramowanie EDR zostanie zainstalowane i skonfigurowane zgodnie z wymaganiami punktów 26 i 44-53 dokumentu.</li> <li>○ <b>Oprogramowanie do kategoryzacji i archiwizacji logów:</b> To narzędzie będzie służyć do gromadzenia, analizowania i przechowywania logów z infrastruktury IT.</li> </ul> </li> <li>• <b>Konfiguracja karty zarządzania:</b> Karta zarządzania serwerem zostanie skonfigurowana w sposób umożliwiający zdalny dostęp i zarządzanie niezależnie od zainstalowanego systemu operacyjnego.</li> <li>• <b>Testy i weryfikacja:</b> Po zakończeniu wdrożenia przeprowadzone zostaną testy weryfikujące poprawność działania wszystkich funkcjonalności serwerów.</li> <li>• <b>Szkolenie:</b> Przeprowadzone zostanie szkolenie personelu Zamawiającego z obsługi i administracji serwerami.</li> </ul>	
<b>2. SERWER TYP II (1 szt.)</b>	
<p>Wdrożenie serwera typu II przebiega analogicznie do wdrożenia serwerów typu I, z uwzględnieniem następujących różnic:</p> <ul style="list-style-type: none"> <li>• Oprogramowanie do monitorowania, spełniające wymagania punktów 20-21 dokumentu, powinno obejmować dodatkowo: <ul style="list-style-type: none"> <li>○ <b>Funkcjonalność wirtualnego asystenta opartego o algorytmy GenAI:</b> Wirtualny asystent będzie wspierał administratorów w analizie danych z monitoringu i identyfikacji potencjalnych zagrożeń.</li> <li>○ <b>Analizę danych z monitoringu pod kątem wykrywania ataków ransomware:</b> System będzie aktywnie poszukiwał wzorców charakterystycznych dla ataków ransomware, minimalizując ryzyko utraty danych.</li> </ul> </li> <li>• <b>Oprogramowanie antywirusowe:</b> Szczegółowe wymagania dotyczące oprogramowania antywirusowego dla serwera typu II opisane są w punktach 75-142 dokumentu.</li> <li>• <b>Oprogramowanie EDR:</b> Instalacja i konfiguracja oprogramowania EDR dla serwera typu II musi spełniać wymagania opisane w punktach 150-183 dokumentu.</li> </ul>	SPEŁNIA TAK /NIE
<b>3. ACCESS POINT (7 szt.)</b>	
<p>Wdrożenie punktów dostępowych obejmuje:</p> <ul style="list-style-type: none"> <li>• <b>Dostawa i instalacja:</b> Dostarczonych zostanie 7 punktów dostępowych, które zostaną zainstalowane w wyznaczonych miejscach w infrastrukturze Zamawiającego.</li> <li>• <b>Konfiguracja:</b> Punkty dostępowe zostaną skonfigurowane do pracy w trybie "cienkiego" punktu dostępowego, zarządzanego z poziomu kontrolera sieci bezprzewodowej. Konfiguracja obejmie m.in. ustawienia sieci bezprzewodowej (SSID, hasło), przypisanie do odpowiednich VLANów oraz integrację z systemem centralnego zarządzania.</li> <li>• <b>Integracja:</b> Punkty dostępowe zostaną zintegrowane z istniejącą infrastrukturą sieciową Zamawiającego.</li> <li>• <b>Szkolenie:</b> Personel Zamawiającego zostanie przeszkolony z podstawowej obsługi punktów dostępowych.</li> </ul>	SPEŁNIA TAK /NIE

4-8. - PRZEŁĄCZNIKI TYP I - V	
Wdrożenie przełączników typów I-V obejmuje:	SPEŁNIA TAK /NIE
• <b>Dostawa i instalacja:</b> Dostarczone zostaną przełączniki odpowiednich typów, które zostaną zainstalowane w wyznaczonych miejscach w infrastrukturze Zamawiającego. Ilość sztuk każdego typu przełącznika jest określona w specyfikacji	
• <b>Konfiguracja:</b> Konfiguracja przełączników obejmuje:	
○ <b>Konfigurację portów i VLANów:</b> Przypisanie portów do odpowiednich VLANów, konfiguracja trunków, agregacja portów.	
○ <b>Konfigurację protokołów routingu:</b> Konfiguracja routingu statycznego i dynamicznego (OSPF).	
○ <b>Konfigurację funkcji bezpieczeństwa:</b> Konfiguracja Stateful Firewall, Policy Based Routing, kontrola dostępu do sieci (ACL), ochrona przed atakami DDoS.	
• <b>Integracja:</b> Przełączniki zostaną zintegrowane z dostarczonym UTM	
• <b>Szkolenie:</b> Personel Zamawiającego zostanie przeszkolony z podstawowej obsługi przełączników.	
9. FIREWALL SPRZĘTOWY (1 szt.)	
Wdrożenie firewalla sprzętowego obejmuje:	SPEŁNIA TAK /NIE
• <b>Dostawa i instalacja:</b> Dostarczony zostanie firewall sprzętowy, który zostanie zainstalowany w wyznaczonym miejscu w infrastrukturze Zamawiającego.	
• <b>Konfiguracja:</b> Konfiguracja firewalla obejmuje wszystkie aspekty jego działania, w tym:	
○ <b>Tryb pracy:</b> Konfiguracja trybu pracy firewalla (router z NAT, transparentny, monitorowanie na porcie SPAN).	SPEŁNIA TAK /NIE
○ <b>Funkcje sieciowe:</b> Konfiguracja filtrowania adresów MAC, NAT, DHCP, VLAN, QoS, VPN, routingu.	
○ <b>Funkcje bezpieczeństwa:</b> Konfiguracja antywirusa, anti-spyware, ochrony przed phishingiem, kontroli aplikacji, sandbox, filtrowania URL, Deep Packet Inspection, SSL Inspection, ochrony DDoS, IPS, zarządzania użytkownikami.	
○ <b>Uwierzytelnianie użytkowników:</b> Konfiguracja mechanizmów uwierzytelniania użytkowników.	
○ <b>Logowanie:</b> Konfiguracja systemu logowania.	
• <b>Integracja:</b> Firewall zostanie zintegrowany z istniejącą infrastrukturą sieciową Zamawiającego.	
• <b>Szkolenie:</b> Personel Zamawiającego zostanie przeszkolony z obsługi i administracji firewallem.	
10. NAS TYP I (1 szt.)	
Wdrożenie serwera NAS typu I obejmuje:	SPEŁNIA TAK /NIE
• <b>Dostawa i instalacja:</b> Dostarczony zostanie serwer NAS w obudowie Rack 2U, który zostanie zainstalowany w wyznaczonym miejscu w infrastrukturze Zamawiającego.	
• <b>Konfiguracja:</b> Konfiguracja serwera NAS obejmuje:	
○ <b>Macierz RAID:</b> Konfiguracja odpowiedniej macierzy RAID w celu zapewnienia redundancyjności i bezpieczeństwa danych.	
○ <b>Protokoły sieciowe:</b> Konfiguracja protokołów sieciowych, takich jak TCP/IP, SMB/CIFS, NFS, FTP.	
○ <b>System wersjonowania plików:</b> Konfiguracja systemu wersjonowania plików, umożliwiającego śledzenie zmian i przywracanie poprzednich wersji plików.	
○ <b>Mechanizmy bezpieczeństwa:</b> Konfiguracja mechanizmów bezpieczeństwa, takich jak kontrola dostępu, szyfrowanie danych, antywirus.	
• <b>Integracja:</b> Serwer NAS zostanie zintegrowany z istniejącą infrastrukturą sieciową Zamawiającego.	SPEŁNIA TAK /NIE
• <b>Szkolenie:</b> Personel Zamawiającego zostanie przeszkolony z obsługi i administracji serwerem NAS.	
11. NAS TYP II (1 szt.)	
Wdrożenie serwera NAS typu II obejmuje:	SPEŁNIA TAK /NIE
• <b>Dostawa i instalacja:</b> Dostarczony zostanie serwer NAS w obudowie Rack 1U, który zostanie zainstalowany w wyznaczonym miejscu w infrastrukturze Zamawiającego.	
• <b>Konfiguracja:</b> Konfiguracja serwera NAS obejmuje:	

<ul style="list-style-type: none"><li>o <b>Macierz RAID:</b> Konfiguracja odpowiedniej macierzy RAID w celu zapewnienia redundancji i bezpieczeństwa danych.</li><li>o <b>Protokoły sieciowe:</b> Konfiguracja protokołów sieciowych, takich jak TCP/IP, SMB/CIFS, NFS, FTP.</li><li>o <b>System kopii zapasowych:</b> Konfiguracja systemu kopii zapasowych, umożliwiającego automatyczne tworzenie kopii zapasowych danych z serwera NAS.</li><li>o <b>Klaster wysokiej dostępności (HA):</b> Konfiguracja klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Klaster musi obsługiwać automatyczne przełączanie awaryjne bez ingerencji administratora.</li><li>o <b>Mechanizmy bezpieczeństwa:</b> Konfiguracja mechanizmów bezpieczeństwa, takich jak kontrola dostępu, szyfrowanie danych, antywirus.</li><li>• <b>Integracja:</b> Serwer NAS zostanie zintegrowany z istniejącą infrastrukturą sieciąową Zamawiającego.</li><li>• <b>Szkolenie:</b> Personel Zamawiającego zostanie przeszkolony z obsługi i administracji serwerem NAS.</li></ul>	
<b>12. OPROGRAMOWANIE DO ARCHIWIZACJI LOGÓW</b>	
<p>Wdrożenie oprogramowania do archiwizacji logów obejmuje:</p> <ul style="list-style-type: none"><li>• <b>Instalacja i konfiguracja:</b> Oprogramowanie zostanie zainstalowane i skonfigurowane na dedykowanym serwerze lub w środowisku wirtualnym Zamawiającego.</li></ul>	SPEŁNIA TAK /NIE
<ul style="list-style-type: none"><li>• <b>Konfiguracja:</b> Konfiguracja oprogramowania obejmie:</li></ul>	
<ul style="list-style-type: none"><li>o <b>Źródła logów:</b> Definicja źródeł logów, z których oprogramowanie będzie zbierać dane (Syslog, Trap SNMP, Windows Event Log).</li></ul>	
<ul style="list-style-type: none"><li>o <b>Powiadamianie:</b> Ustawienia powiadamiania o ważnych zdarzeniach.</li></ul>	
<ul style="list-style-type: none"><li>o <b>Polityki retencji danych:</b> Konfiguracja polityk retencji danych, określających jak długo logi będą przechowywane.</li></ul>	
<ul style="list-style-type: none"><li>• <b>Szkolenie:</b> Personel Zamawiającego zostanie przeszkolony z obsługi i administracji oprogramowaniem.</li><li>• <b>Usługa wdrożenia:</b> W zakresie usługi wdrożenia zapewniona zostanie instalacja, konfiguracja, szkolenie i wsparcie.</li></ul>	
<b>13 -14 OPROGRAMOWANIE DO TWORZENIA KOPII ZAPASOWYCH NA POTRZEBY URZĘDU i OPS</b>	
<p><b>Cel wdrożenia</b></p> <p>Celem wdrożenia jest implementacja systemu do zarządzania kopiami zapasowymi, który zapewni ochronę kluczowych danych urzędu oraz jednostek organizacyjnych. Rozwiązanie ma umożliwić centralne zarządzanie procesami tworzenia i odtwarzania kopii zapasowych, zwiększając poziom bezpieczeństwa informacji i zgodność z obowiązującymi przepisami, w tym RODO.</p>	SPEŁNIA TAK /NIE
<p><b>Zakres prac wdrożeniowych</b></p> <p><b>1. Analiza przedwdrożeniowa</b></p> <ul style="list-style-type: none"><li>• Przegląd istniejącej infrastruktury IT w siedzibie Zamawiającego.</li><li>• Ocena aktualnego stanu zabezpieczeń danych oraz procesów backupowych.</li><li>• Identyfikacja krytycznych zasobów objętych kopią zapasową, takich jak stacje robocze, serwery i bazy danych.</li><li>• Opracowanie planu wdrożenia uwzględniającego specyfikę środowiska IT i potrzeby Zamawiającego.</li></ul>	
<p><b>2. Instalacja i konfiguracja systemu</b></p> <ul style="list-style-type: none"><li>• <b>Serwer centralny:</b><ul style="list-style-type: none"><li>o Instalacja oprogramowania zarządzającego na dedykowanym serwerze w środowisku fizycznym lub wirtualnym.</li><li>o Konfiguracja magazynu kopii zapasowych z zapewnieniem redundancji danych.</li><li>o Ustawienie parametrów zabezpieczeń, takich jak szyfrowanie i segmentacja dostępu.</li></ul></li><li>• <b>Stacje klienckie i serwery:</b><ul style="list-style-type: none"><li>o Zdalna instalacja modułów klienckich na urządzeniach objętych procesem backupu.</li></ul></li></ul>	

<ul style="list-style-type: none"> <li>○ Ustawienie polityk backupowych, takich jak harmonogramy zadań, retencja danych oraz zakres ochrony.</li> <li>○ Optymalizacja obciążenia sieci lokalnej i magazynu danych poprzez zastosowanie kompresji i backupu różnicowego/przyrostowego.</li> </ul>	
<b>3. Testowanie funkcjonalności</b> <ul style="list-style-type: none"> <li>• Przeprowadzenie testowych kopii zapasowych, w tym pełnych, różnicowych i delta, aby zweryfikować poprawność działania systemu.</li> <li>• Odtworzenie danych z testowych kopii zapasowych, w tym: <ul style="list-style-type: none"> <li>○ Symulacja odzyskiwania plików, folderów i całych systemów operacyjnych.</li> <li>○ Weryfikacja procedur przywracania danych na nowe urządzenia (bare metal restore).</li> </ul> </li> <li>• Testy wydajnościowe w rzeczywistych warunkach użytkowania, z uwzględnieniem równoczesnych operacji backupu wielu urządzeń.</li> </ul>	
<b>1. Szkolenie administratorów</b> <ul style="list-style-type: none"> <li>• Szkolenie personelu IT w zakresie: <ul style="list-style-type: none"> <li>○ Konfiguracji i zarządzania systemem kopii zapasowych.</li> <li>○ Monitorowania zadań i interpretacji raportów oraz alertów.</li> <li>○ Procedur odzyskiwania danych w sytuacjach awaryjnych.</li> </ul> </li> <li>• Przekazanie instrukcji użytkownika oraz dokumentacji technicznej.</li> </ul>	
<b>5. Uruchomienie produkcyjne</b> <ul style="list-style-type: none"> <li>• Wdrożenie w środowisku produkcyjnym w sposób minimalizujący wpływ na bieżącą działalność urzędu.</li> <li>• Bieżące monitorowanie pierwszych zadań backupowych w celu zapewnienia ich poprawności.</li> </ul> Przekazanie systemu Zamawiającemu wraz z pełną dokumentacją i raportem z realizacji wdrożenia	
<b>16- DYSKI DO MACIERZY 14 SZT</b>	
<b>1. Przygotowanie macierzy</b> <ul style="list-style-type: none"> <li>• Przed rozpoczęciem instalacji sprawdzana jest zgodność systemowa i aktualny stan firmware macierzy, aby zapewnić pełną kompatybilność z nowymi dyskami SSD.</li> <li>• Weryfikowana jest dostępność odpowiedniej liczby wnęk na dyski w macierzy.</li> <li>•</li> </ul>	SPEŁNIA TAK /NIE
<b>2. Instalacja dysków SSD</b> <ul style="list-style-type: none"> <li>• Dyski są instalowane w macierzy w wyznaczonych slotach zgodnie z dokumentacją techniczną.</li> <li>• Proces instalacji realizowany jest bez przerywania pracy urządzenia (hot-swap), co minimalizuje wpływ na bieżącą działalność urzędu.</li> </ul>	
<b>3. Konfiguracja logiczna</b> <ul style="list-style-type: none"> <li>• Po instalacji dysków wykonywana jest ich integracja z istniejącą konfiguracją macierzy.</li> <li>• Tworzone są nowe pule pamięci lub rozszerzane istniejące, w zależności od potrzeb Zamawiającego.</li> <li>• Konfiguracja poziomów RAID zapewnia optymalną równowagę między wydajnością, bezpieczeństwem i dostępnością danych.</li> </ul>	
<b>4. Testy działania</b> <ul style="list-style-type: none"> <li>• Przeprowadzane są testy wydajnościowe i funkcjonalne w celu weryfikacji poprawności instalacji.</li> <li>• Testowane jest odczytywanie, zapisywanie i replikacja danych w środowisku urzędu.</li> </ul>	

Niespełnienie któregokolwiek z wymaganych parametrów oraz wymagań co do nich wartości minimalnych spowoduje odrzucenie oferty bez dalszej jej oceny jako oferta niezgodna z warunkami zamówienia.