Załącznik nr 1 do SWZ

Opis Przedmiotu Zamówienia

Oprogramowanie oraz infrastruktura sprzętowa

Spis treści

WSTĘP

Niniejszy załącznik określa minimalne wymagania dla dostawy/wdrożenia/uruchomienia oprogramowania oraz infrastruktury sprzętowej dla Powiatu Nowotomyskiego realizowanego w ramach „Cyberbezpieczny Samorząd" dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Celem projektu jest zwiększenia poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego.

ETAP I

1. PRZEŁĄCZNIKI SIECIOWE L3 NA POTRZEBY PODGIK

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zakup 2 szt. przełączników sieciowych L3 z modułem stack wraz z konfiguracją, instruktarzem stanowiskowym i wsparciem serwisowym na potrzeby PODGiK
Interfejsy	Przełącznik musi posiadać minimum 48 portów dostępowych Ethernet 10/100/1000 Auto-MDI/MDIX. Każdy w portów musi obsługiwać PoE+ (do 30W per interfejs). Przełącznik musi posiadać nie mniej niż 4 porty uplink 10 Gigabit Ethernet SFP+. Korzystanie z portów uplink nie może powodować wyłączenia portów dostępowych 10/100/1000. Porty uplink muszą akceptować również wkładki SFP umożliwiając obsługę połączeń uplink Gigabit Ethernet. Przełącznik musi posiadać nie mniej niż 2 porty uplink o prędkości 40 Gb/s na wkładki typu QSFP+. Przełącznik musi umożliwiać stworzenie stosu (w postaci pętli) liczącego nie mniej niż 10 urządzeń. Dopuszczalne jest podłączanie do stosu portami uplink 10 Gb/s lub 40 Gb/s. Stos musi być widoczny z punktu widzenia zarządzania oraz innych urządzeń sieciowych jako jedno urządzenie. Zarządzanie wszystkimi przełącznikami w stosie musi się odbywać z dowolnego przełącznika będącego częścią stosu. Stos musi być odporny na awarie, tzn. przełącznik kontrolujący pracę stosu (master) musi być automatycznie zastąpiony przełącznikiem pełniącym rolę backup'u – wybór przełącznika backup nie może odbywać się w momencie awarii przełącznika master. Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
Pamięć RAM	Przełącznik musi być wyposażony w nie mniej niż 2 GB pamięci Flash oraz 2 GB pamięci DRAM.
Zarządzanie	Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.
Wydajność	Przełącznik musi posiadać architekturę non-blocking. Maksymalna wydajność przełączania w warstwie 2 nie może być niższa niż 330 Gb/s i 250 milionów pakietów na sekundę. Przełącznik nie może obsługiwać mniej niż 32 000 adresów MAC. Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów).
VLAN	Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4093. Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based). W celu automatycznej konfiguracji sieci VLAN, przełącznik musi obsługiwać protokół MVRP.
Obsługa połączeń	Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 128 grup LAG, maksymalnie nie mniej niż 16 linków w grupie.

	Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, zgodnie z IEEE 802.1D i 802.1w, a także Multiple Spanning Tree zgodnie z IEEE 802.1s (nie mniej niż 64 instancje MSTP. Przełącznik musi obsługiwać protokół LLDP i LLDP-MED.
Routing	Urządzenie musi obsługiwać routing między sieciami VLAN – routing statyczny, oraz protokół routingu dynamicznego RIP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 14 000. Przełącznik musi posiadać możliwość uruchomienia protokołów routingu dynamicznego, dla IPv4 (nie mniej niż OSPF i BGP) oraz dla IPv6 (nie mniej niż OSPFv3 i RIPng). Jeżeli ww. funkcjonalność jest dodatkowo licencjonowana należy wraz z urządzeniem dołączyć taką licencję.
Funkcjonalność dodatkowa	Urządzenie musi posiadać możliwość obsługi funkcji PIM sparse mode, PIM source specific mode (PIM-SSM), IGMP v1, v2, v3, oraz MLD v1 i v2. Jeżeli ww. funkcjonalność jest dodatkowo licencjonowana należy wraz z urządzeniem dołączyć taką licencję. Urządzenie musi posiadać możliwość uruchomienia Ethernet OAM link fault management (LFM). Jeżeli ww. funkcjonalność jest dodatkowo licencjonowana należy wraz z urządzeniem dołączyć taką licencję. Urządzenie musi pozwalać na zarządzanie po IPv6. Urządzenie musi posiadać mechanizmy priorytetyzowania dla ruchu wchodzącego i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny. Urządzenie musi obsługiwać filtrowanie ruchu na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo nie mniej niż 1500 reguł filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu. Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping. Przełącznik musi obsługiwać IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. Przełącznik musi obsługiwać co najmniej następujące typy EAP: MD5, TLS, TTLS, PEAP. Urządzenie musi obsługiwać protokół SNMP (wersje 2 i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN. Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów

	musi być oddzielony od modułu routingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem. Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 20 poprzednich, kompletnych konfiguracji.
Opieka techniczna, autoryzacja	Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej przez okres minimum 36 miesięcy. Opieka musi zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu, wymianę uszkodzonego sprzętu w ciągu 5 dni, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego przez producenta kanału sprzedaży, na terenie Unii Europejskiej – do oferty należy dołączyć oświadczenie producenta lub autoryzowanego dystrybutora sprzętu poświadczające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.
Wdrożenie	Oferent zobowiązany jest do konfiguracji urządzeń w zakresie co najmniej istniejących VLAN'ów (10 szt.) na podstawie konfiguracji urządzeń istniejących (switche DCN) i uruchomienia pracy obu nowych urządzeń w trybie stack. Powyższe ma za zadanie firzyczne uruchomienie, konfiguracje j/w, w celu zachowania ciągłości pracy w wydziale.
Szkolenie z obsługi	Wymagane jest także zapewnienie szkolenia z zakresu konfiguracji i zarządzania urządzenia. Szkolenie musi być przeprowadzone dla minimum 2 osób w języku polskim.
Zasilanie	Urządzenie musi być wyposażone w zasilacz i posiadać możliwość wyposażenia w zapasowy zasilacz.
Ilość	1 kpl.

2. URZĄDZENIE KLASY UTM NA POTRZEBY PODGIK

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zakup i wdrożenie UTM na potrzeby PODGiK: zestawienie klastra z istniejącym urządzeniem Foritgate 70F
Wymagania ogólne	Wymagania Ogólne 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.

	System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. 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. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. Redundancja, monitoring i wykrywanie awarii 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. Interfejsy, Dysk, Zasilanie: 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów minimum: • 10 portami Gigabit Ethernet RJ-45. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC. Parametry wydajnościowe: 1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps. 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 1.3 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 750 Mbps.

	7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 650 Mbps. Funkcje Systemu Bezpieczeństwa: W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). Polityki, Firewall 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

	7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Połączenia VPN 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • 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. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. • 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. Routing i obsługa łączy WAN W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.

	4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. Funkcje SD-WAN 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). Zarządzanie pasmem 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. Ochrona przed malware 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. 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. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

	9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. Ochrona przed atakami 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. Kontrola aplikacji 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). Kontrola WWW

	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. Uwierzytelnianie użytkowników w ramach sesji 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. Zarządzanie 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.

	3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. Logowanie 1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. 7. Możliwość rozbudowania Systemu o dodatkowe usługi: logowania, raportowania, korelacji zdarzeń realizowanych w chmurze. Testy wydajnościowe oraz funkcjonalne Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy. Serwisy i licencje Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza

	typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na na okres 24 miesięcy
Gwarancja i serwis	System jest objęty serwisem gwarancyjnym producenta przez minimum 24 miesiące. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Wdrożenie	Wykonawca ma za zadanie utworzenie klastra z istniejącym w wydziale urządzeniem Foritgate-70F. Zadanie to powinno zostać wykonane w możliwie krótkim czasie, w celu zachowania ciągłości pracy wydziału.
Ilość	1 szt.

3. OPROGRAMOWANIE DO ARCHIWIZOWANIA DANYCH NA POTRZEBY PODGIK

Nazwa	**Minimalne wymagania dla oprogramowania**
Typ	Zakup oprogramowania do archiwizowania danych, raportowania, zbierania informacji na temat działania sieci na potrzeby PODGIK
Wymagania Ogólne	• W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. • Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia
Interfejsy, Dysk	System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności minimum 3 TB.
Parametry wydajnościowe:	• System musi być w stanie przyjmować minimum 5 GB logów na dzień. • Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.
Wymagania szczegółowe	W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje: Logowanie: • Podgląd logowanych zdarzeń w czasie rzeczywistym. • Możliwość przeglądania logów historycznych z funkcją filtrowania. • System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: o Listę najczęściej wykrywanych ataków. o Listę najbardziej aktywnych użytkowników. o Listę najczęściej wykorzystywanych aplikacji. o Listę najczęściej odwiedzanych stron www. o Listę krajów, do których nawiązywane są połączenia.

	○ Listę najczęściej wykorzystywanych polityk Firewall. ○ Informacje o realizowanych połączeniach IPSec. • Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. • Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. • System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy. Raportowanie: W zakresie raportowania system musi zapewniać: • Generowanie raportów co najmniej w formatach: PDF, CSV. • Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. • Funkcję definiowania własnych raportów. • Możliwość spolszczenia raportów. • Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. Korelacja logów: W zakresie korelacji zdarzeń system musi zapewniać: 1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie vpn, utracone połączenie sieciowe. • Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie. Zarządzanie: • System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która

	komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. • Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. • System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. Serwisy i licencje: • System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. 2. Wsparcie: System musi być objęty serwisem producenta do dnia 30.06.2026 r, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
Ilość	1 szt.

4. SERWER NAS NA POTRZEBY PCPR

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zakup serwera NAS do gromadzenia danych oraz backup zawierającego dyski oraz kartę sieciową, obsługującego system raid wraz z montażem, konfiguracją i wsparciem serwisowym dla PCPR
Procesor	Procesor 64 bit x86 o taktowaniu nie mniejszym niż 2.8 GHz
Procesor liczba rdzeni	Nie mniej niż 8
Pamięć RAM	Nie mniej niż 8GB
Pamieć RAM liczba slotów	Minimum 2 sloty
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 64GB
Pamięć Flash	Nie mniej niż 5GB
Gniazdo M.2	Minimum 2
Liczba zatok na dyski twarde	Minimum 8
Obsugiwane dyski twarde	3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" SSD SATA
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 1
Porty LAN 2,5 GbE	Minimum 2
Diody LED	Minimum Stan, LAN, HDD, USB
Porty USB 3.2 Gen 1	Minimum 4
Port PCiE	Tak, minimum 2 Gen3
Typ obudowy	RACK, maksymalnie 2U

Zasilanie	Zasilacz max. 250W, 100-240 V
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Funkcje backup	Oprogramowanie do tworzenia kopii plików, opracowane przez producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android
VPN	VPN client / VPN server. Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania

	Kopia zapasowa ustawień/przywracanie ustawień/resetowanie ustawień systemu
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Gwarancja	Minimum 36 miesięcy
Zainstalowane dyski	Minimum 6 sztuk dysków, minimum 6TB 3,5” SATA
Wdrożenie	Wdrożenie w zakresie : Dostawa Montaż fizyczny Uruchomienie Wstępna konfiguracja zgodna z wytycznymi zamawiającego Zamawiający wymaga montażu fizycznych serwerów wraz z pełną aktualizacją systemu operacyjnego hosta oprogramowania układowego serwera na dzień wdrożenia. wymagane jest zaadresowanie interfejsu niskopoziomowego zarządzania, oraz serwera fizycznego Parametry zostaną podane na etapie realizacji wdrożenia. Wdrożenie musi być zakończone dokumentacją powdrożeniową opisującą wszelkie istotne w punktu działania klastra rekonfigurację, w tym opis konfiguracji konsoli niskopoziomowego zarządzania serwerem.
Ilość	1 szt.

5. ZASILACZ AWARYJNY UPS NA POTRZEBY PCPR

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zakup zasilacza awaryjnego rakowego - UPS na potrzeby PCPR
Parametry techniczne	• Topologia UPS: On-Line • Moc (W): minimum 5400 W • Moc (VA): minimum 6000 VA • Ilość gniazd wyjściowych: minimum 1 szt • Złącze wejściowe: Kostka zaciskowa • Złącze wyjściowe: Kostka zaciskowa • Kształt fali przy pracy baterii: Czysta fala sinusoidalna • Kompatybilność z aktywnym PFC: tak • Zabezpieczenie przeciwprzepięciowe: tak • Port wyłącznika awaryjnego (EPO): tak • Faza: 1 Fazowe

	• Dodatkowy moduł bateryjny: tak • Zdalne monitorowanie SNMP / HTTP: tak • Port USB zgodny z HID: tak • Panel LCD: tak
Gwarancja	Minimum 24 miesiące gwarancji producenta
Ilość	1 szt.

6. OPROGRAMOWANIE ANTYWIRUSOWE NA POTRZEBY PCPR

Nazwa	**Minimalne wymagania dla oprogramowania**
Typ	Zakup oprogramowania antywirusowego zapewniającego wielowarstwową ochronę stacji roboczych oraz systemów chmurowych wraz z oprogramowaniem EDR z licencją i wsparciem serwisowym na potrzeby PCPR
Wymagania ogólne	Zamawiający wymaga dostarczenia licencji obejmującej minimum 30 użytkowników, na okres do 30-06-2026 r.
Wymagania szczegółowe	Administracja zdalna w chmurze 1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.

	12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. Ochrona stacji roboczych 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi integrować się z Intel Threat Detection Technology. 11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.

	Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 26. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 27. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 28. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 29. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 30. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 31. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

	Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. Ochrona serwera 32. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux 33. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 34. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 35. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 36. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 37. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 38. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 39. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. Dodatkowe wymagania dla ochrony serwerów Windows: 40. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej 41. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 42. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 43. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 44. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

	45. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 46. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 47. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 48. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe wymagania dla ochrony serwerów Linux: 49. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 50. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 51. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, 52. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. Szyfrowanie 53. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11. 54. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 55. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 56. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. Ochrona urządzeń mobilnych opartych o system Android 57 Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 58 Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 59 Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 60 Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: usunięcie zawartości urządzenia,

	przywrócenie urządzenie do ustawień fabrycznych, zablokowania urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła. Sandbox w chmurze 61. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 62. Rozwiązanie musi wykorzystywać do działania chmurę producenta. 63. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 64. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 65. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. 66. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 67. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. 68. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. 69. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 70. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. 71. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. a. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: Czysty, b. Podejrzany, c. Bardzo podejrzany, d. Szkodliwy. 72. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

	73. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. 74. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia. Moduł XDR 75. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 76. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 77. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 78. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 79. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. 80. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. 81. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 82. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. 83. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 84. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 85. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 86. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. 87. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. 88. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących

	przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. 89. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich. 90. Konsola administracyjna musi mieć możliwość tagowania obiektów. 91. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
Ilość	1 szt.

7. OPROGRAMOWANIE ZAPEWNIAJĄCE WIELOWARSTWOWĄ OCHRONĘ DLA PUP

Nazwa	**Minimalne wymagania dla oprogramowania**
Typ	Zakup oprogramowania zapewniającego wielowarstwową ochronę stacji roboczych oraz serwerów plikowych i pocztowych, obejmujących antywirus, antyspyware, personal firewall, antyspam, filtr treści z licencją i wsparciem dla PUP
Wymagania ogólne	Zamawiający wymaga dostarczenia licencji obejmującej minimum 30 użytkowników, na okres do 30-06-2026 r.
Wymagania szczegółowe	Administracja zdalna w chmurze 1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z

	funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. Ochrona stacji roboczych 16. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 17. Rozwiązanie musi wspierać architekturę ARM64. 18. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 19. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 20. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 21. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 22. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 23. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 24. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 25. Rozwiązanie musi integrować się z Intel Threat Detection Technology. 26. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 27. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 28. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej

	inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 29. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 30. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 32. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 33. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 34. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 35. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 36. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 37. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

	tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. Ochrona serwera 40. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. 41. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 42. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 43. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 44. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 45. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 46. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 47. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. Dodatkowe wymagania dla ochrony serwerów Windows:

	49. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej . 50. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 51. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 52. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 53. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 54. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 55. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 56. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 57. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe wymagania dla ochrony serwerów Linux: 53. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 54. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 55. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, 56. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. Szyfrowanie 57. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11. 58. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 59. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.

	60. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. Ochrona urządzeń mobilnych opartych o system Android 61 Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 62 Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 63 Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 64 Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: usunięcie zawartości urządzenia, przywrócenie urządzenie do ustawień fabrycznych, zablokowania urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła. Sandbox w chmurze 64. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 65. Rozwiązanie musi wykorzystywać do działania chmurę producenta. 66. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 66. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 67. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. 67. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 68. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.

	69. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. 72. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 73. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. 74. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. a. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: Czysty, b. Podejrzany, c. Bardzo podejrzany, d. Szkodliwy. 75. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. 76. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. 77. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia. Moduł XDR 92. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 93. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 94. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 95. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 96. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. 97. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. 98. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 99. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.

	100. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 101. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 102. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 103. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. 104. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. 105. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. 106. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich. 107. Konsola administracyjna musi mieć możliwość tagowania obiektów. 108. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
Ilość	1 szt.

8. OPROGRAMOWANIE DO BACKUPU DLA PUP

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Zakup oprogramowania z narzędziami służącymi do backupu, replikacji oraz zarządzania danymi w środowiskach wirtualnych i chmurowych, pozwalających na tworzenie kopii zapasowych i przywracanie danych z licencją i wsparciem dla PUP

Parametry techniczne	• Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. • Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL (w tym odtwarzanie point-in-time). • Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania. • Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych. • Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn. • Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. • Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites. • Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska. • Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska. • Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn . • Oprogramowanie musi wspierać granularne odtwarzanie baz danych z opcją odtwarzanie point-in-time wraz. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. • Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego. • Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i HyperV używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. • Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. • Testy muszą być przeprowadzone bez interakcji z administratorem. • Oprogramowanie musi mieć podobne mechanizmy dla replik.

	• Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. • System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego • System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. • System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii • System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn. • System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz XLS. • System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora. • System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów. • System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard). • System musi wspierać wiele instancji jednocześnie bez konieczności instalowania dodatkowych modułów. • System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach. • System musi mieć możliwość eksportowania raportów do formatów DOC, XLS, PDF. • Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego. • Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych. • Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux • Rozwiązanie musi wspierać systemy operacyjne macOS. • Rozwiązanie musi wspierać wykonywanie kopi zapasowych następujących systemów plików: NTFS, ReFS, FAT32, ext2, ext3, ext4, ReiserFS, JFS, XFS, F2FS, Brtfs (dla kernela 3.16 i nowszych), APFS, HFS, HFS+, NILFS2. • Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą).

	• Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster. • Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów. • Rozwiązanie musi wspierać backup podłączonych dysków USB. • Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym. • Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na: • Lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, • Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, • Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub • NFS, • Zcentralizowanym repozytorium danych, • Bezpośrednio na zasobach Chmury. • Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone. • Rozwiązanie musi wspierać kontrolę pasma sieciowego. • Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych. • Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN. • Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft. • Rozwiązanie musi wspierać skrypty wykonywane przed i po wykonaniu zadania oraz przed i po wykonaniu migawki na poziomie wolumenu. • Rozwiązanie musi wspierać technologię BitLocker. • Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania. • Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych. • Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL poprzez bezpośrednie uruchomienie ich z pliku backupu. • Rozwiązanie musi wspierać szyfrowanie. • Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne. • Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego. • Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.

	Powyższa funkcjonalność ma działać w środowisku wirtualnym i/lub fizycznym. Wymagane jest dostarczenie licencji wieczystych dla zabezpieczenia minimum 5 sztuk wirtualnych i/lub fizycznych serwerów oraz minimum 25 maszyn roboczychWraz z oprogramowanie wymagane jest dostarczenie wsparcia producenta oprogramowania do 30-06-2026 r.
Ilość	1 szt.

9. SERWER NAS NA POTRZEBY PUP

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zakup serwera NAS do gromadzenia danych oraz backup zawierającego dyski, obsługującego system raid wraz z montażem,konfiguracją i wsparciem serwisowym na potrzeby PUP
Procesor	Procesor 64 bit x86 o takowaniu nie mniejszym niż 2.8 GHz
Procesor liczba rdzeni	Nie mniej niż 8
Pamięć RAM	Nie mniej niż 8GB
Pamieć RAM liczba slotów	Minimum 2 sloty
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 64GB
Pamięć Flash	Nie mniej niż 5GB
Gniazdo M.2	Minimum 2
Liczba zatok na dyski twarde	Minimum 8
Obsugiwane dyski twarde	3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" SSD SATA
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 1
Porty LAN 2,5 GbE	Minimum 2
Diody LED	Minimum Stan, LAN, HDD, USB
Porty USB 3.2 Gen 1	Minimum 4
Port PCiE	Tak, minimum 2 Gen3
Typ obudowy	RACK, maksimum 2U
Zasilanie	Zasilacz max. 250W, 100-240 V
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID

	Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Funkcje backup	Oprogramowanie do tworzenia kopii plików, opracowane przez producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android
VPN	VPN client / VPN server. Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Kopia zapasowa ustawień/przywracanie ustawień/resetowanie ustawień systemu
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS

Gwarancja	Minimum 36 miesięcy
Zainstalowane dyski	Minimum 6 sztuk dysków, minimum 6TB 3,5” SATA
Wdrożenie	Wdrożenie w zakresie : Dostawa Montaż fizyczny Uruchomienie Wstępna konfiguracja zgodna z wytycznymi zamawiającego Zamawiający wymaga montażu fizycznych serwerów wraz z pełną aktualizacją systemu operacyjnego hosta oprogramowania układowego serwera na dzień wdrożenia. wymagane jest zaadresowanie interfejsu niskopoziomowego zarządzania, oraz serwera fizycznego Parametry zostaną podane na etapie realizacji wdrożenia. Wdrożenie musi być zakończone dokumentacją powdrożeniową opisującą wszelkie istotne w punktu działania klastra rekonfigurację, w tym opis konfiguracji konsoli niskopoziomowego zarządzania serwerem.
Ilość	1 szt.

10. SERWER Z PRZEZNACZENIEM DO WIRTUALIZACJI NA POTRZEBY PUP

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zakup serwera z przeznaczeniem do wirtualizacji systemów zawierającego dyski, z obsługą raid oraz oprogramowaniem wraz z konfiguracją, licencją i wsparciem serwisowym - na potrzeby PUP
Obudowa	• Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. • Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów minimum 32 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowane minimum dwa procesory min. 8-rdzeniowe, taktowane min. 2.9GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 175 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. Wydruk z

	testu należy dołączyć do oferty. Zamawiający dopuszcza wydruk w języku angielskim.
RAM	• Minimum 256GB pamięci RDIMM 5600MT/s, • Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.
Funkcjonalność pamięci RAM	• Demand Scrubing, • Patrol Scrubing, • Permanent Fault Detection
Gniazda PCI	• minimum dwa sloty PCIe generacji 5
Interfejsy sieciowe/FC/SAS	• Wbudowane: - min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT - min. 4 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Dyski twarde	Zainstalowane minimum 6 dysków SSD o pojemności minimum 2TB każdy
Wbudowane porty	Minimum 4 x USB z czego nie mniej niż 1x USB 3.0, 2x VGA
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 1100W każdy.
System Operacyjny	Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO, pokrywającego licencyjnie Wszystkie core oferowanych procesorów. Zamawiający wymaga dostarczenia minimum 25 licencji dostępowych dla użytkowników Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym minimum dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru

	energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, III. zdalna dystrybucja oprogramowania na stacje robocze, IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

	1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, VI. szyfrowanie plików i folderów, VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), VIII.możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, IX. serwis udostępniania stron WWW, X. wsparcie dla protokołu IP w wersji 6 (IPv6), XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła

	• Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej; o zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); o szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; o możliwość podmontowania zdalnych wirtualnych napędów; o wirtualną konsolę z dostępem do myszy, klawiatury; o wsparcie dla IPv6; o wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; o integracja z Active Directory; o możliwość obsługi przez dwóch administratorów jednocześnie; o wsparcie dla dynamic DNS; o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. o możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera o możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej o Przesyłanie danych telemetrycznych w czasie rzeczywistym o Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze o Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych o integracja z Active Directory

	○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych,

	występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub równoważne • Serwer musi posiadać deklaracja CE lub normy równoważne
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Min. 36 m-cy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez linię telefoniczną producenta. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. • Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 lub równoważne na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

	Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
Wdrożenie	Zamawiający wymaga montażu fizycznych serwerów wraz z pełną aktualizacją systemu operacyjnego hosta i maszyn wirtualnych/oprogramowania układowego serwera na dzień wdrożenia. Wymagane jest zaadresowanie interfejsu niskopoziomowego zarządzania, oraz serwera fizycznego i maszyn wirtualnych które to Wykonawca musi uruchomić na w/w serwerze. Parametry minimalne w/w maszyn wirtualnych zostaną podane na etapie realizacji wdrożenia. W ramach wdrożenia należy podłączyć dostarczane serwery do dostarczanej macierzy za pomocą dedykowanych przewodów. Zezwala się na połączenie direct między macierzą i serwerem bez wykorzystania dedykowanego przełącznika. W ramach wdrożenia należy wykonać testy redundancji sieci SAN za pomocą fizycznego odpięcia każdej ścieżki. Wdrożenie musi być zakończone dokumentacją powdrożeniową opisującą wszelkie istotne w punktu działania klastra rekonfigurację, w tym opis konfiguracji konsoli niskopoziomowego zarządzania serwerem.
Ilość	1 szt.

11. OPROGRAMOWANIE DO ARCHIWIZOWANIA DANYCH NA POTRZEBY PUP

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Zakup oprogramowania do archiwizowania danych, raportowania, zbierania informacji na temat działania sieci wraz z licencją jako uzupełnienie istniejącego UTM na potrzeby PUP
Wymagania Ogólne	• W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. • Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia
Interfejsy, Dysk	• System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności minimum 3 TB.
Parametry wydajnościowe:	• System musi być w stanie przyjmować minimum 5 GB logów na dzień. • Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

Wymagania szczegółowe	W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje: Logowanie: • Podgląd logowanych zdarzeń w czasie rzeczywistym. • Możliwość przeglądania logów historycznych z funkcją filtrowania. • System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: o Listę najczęściej wykrywanych ataków. o Listę najbardziej aktywnych użytkowników. o Listę najczęściej wykorzystywanych aplikacji. o Listę najczęściej odwiedzanych stron www. o Listę krajów, do których nawiązywane są połączenia. o Listę najczęściej wykorzystywanych polityk Firewall. o Informacje o realizowanych połączeniach IPSec. • Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. • Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. • System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy. Raportowanie: W zakresie raportowania system musi zapewniać: • Generowanie raportów co najmniej w formatach: PDF, CSV. • Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. • Funkcję definiowania własnych raportów. • Możliwość spolszczenia raportów. • Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. Korelacja logów: W zakresie korelacji zdarzeń system musi zapewniać: 12. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 13. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.

	14. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie vpn, utracone połączenie sieciowe. Zarządzanie: • System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. • Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. • System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. Serwisy i licencje: • System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. 2. Wsparcie: System musi być objęty serwisem producenta do 30-06-2026 r. upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
Ilość	1 szt.

12. URZĄDZENIE KLASY UTM NA POTRZEBY PCS

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zakup i wdrożenie UTM na potrzeby PCS wraz z licencją i wsparciem serwisowym
Wymagania szczegółowe	Wymagania Ogólne 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.

	System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. 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. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. Redundancja, monitoring i wykrywanie awarii 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. Interfejsy, Dysk, Zasilanie: 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 5 portami Gigabit Ethernet RJ-45. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC. Parametry wydajnościowe: 1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps. 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 1 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.

	7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps. Funkcje Systemu Bezpieczeństwa: W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). Polityki, Firewall 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

	7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Połączenia VPN 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • 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. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. • 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. Routing i obsługa łączy WAN W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.

	4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. Funkcje SD-WAN 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). Zarządzanie pasmem 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. Ochrona przed malware 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. 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. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

	9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. Ochrona przed atakami 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. Kontrola aplikacji 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). Kontrola WWW

	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. Uwierzytelnianie użytkowników w ramach sesji 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. Zarządzanie 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.

	3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. Logowanie 1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. Testy wydajnościowe oraz funkcjonalne Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy. Serwisy i licencje Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

Gwarancja i serwis	System musi być objęty serwisem gwarancyjnym producenta dna okres minimum 24 miesiące W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Wdrożenie	Zamawiający wymaga przeprowadzenie wdrożenia dostarczonego urządzenia UTM w zakresie minimum: • Wstępna konfiguracja urządzenia UTM/NGFW - dostępy administracyjne, synchronizacja czasu • Przeniesienie konfiguracji z obecnie posiadanego rozwiązania (Reguły firewall/NAT, konfiguracja interfejsów, routing statyczny, DHCP, IPSec VPN do 10 tuneli) • Uruchomienie SSL VPN (wewnętrzna baza użytkowników lub Active Directory/LDAP) • Integracja z Active Directory + Agent SSO • Dostosowanie wyjątków dla alarmów lub zaawansowanej konfiguracji systemu IPS. • Uruchomienie funkcji automatycznego backupu konfiguracji. • Uruchomienie funkcji DNS proxy. • Uruchomienie wbudowanego systemu raportowania. • Uruchomienie powiadomień mailowych • Konfiguracja zbierania logów • Uruchomienie agenta SNMP • Przygotowanie Dokumentacji powdrożeniowej .
Ilość	1 szt.

13. PRZEŁĄCZNIK SIECIOWY L2 NA POTRZEBY PSC

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zakup przełącznika sieciowego L2 na potrzeby PSC wraz z konfiguracją i wsparciem serwisowym
Typ przełącznika	Zarządzany
Podstawowe przełączanie RJ-45 Liczba portów Ethernet	Minimum 24
Podstawowe przełączania Ethernet RJ-45 porty typ	Gigabit Ethernet (10/100/1000)
Ilość portów Gigabit Ethernet	Minimum 24
Ilość slotów Modułu SFP+	Minimum 4
Obsługa 10G	Tak
Obsługa sieci VLAN	Tak

Przepustowość rutowania/przełączania	Minimum 128 Gbit/s
Przepustowość	Minimum 190 Mpps
Układ	Maksimum 1U
Pojemność pamięci wewnętrznej	Minimum 512MB
Wielkość pamięci flash	Minimum 64 MB
Zasilanie PoE	Minimum 185 W
Porty PoE	Minimum 12 (802.3af/at)
Certyfikaty	FCC CE RCM VCCI BSMI UL RoHS2 CB
Gwarancja	Minimum 12 miesięcy gwarancji producenta
Wdrożenie	Wdrożenie w zakresie : Dostawa Montaż fizyczny Uruchomienie Wstępna konfiguracja zgodna z wytycznymi zamawiającego Zamawiający wymaga montażu fizycznych wraz z pełną aktualizacją systemu operacyjnego - W ramach wdrożenia należy podłączyć urządzenia Wdrożenie musi być zakończone dokumentacją powdrożeniową opisującą wszelkie istotne w punktu działania
Ilość	1 szt.

14. OPROGRAMOWANIE ANTYWIRUSOWE NA POTRZEBY PCS

Nazwa	**Minimalne wymagania dla oprogramowania**
Typ	Zakup oprogramowania antywirusowego z licencją dla PCS
Wymagania ogólne	Zamawiający wymaga dostarczenia licencji obejmującej minimum 10 użytkowników, na okres do 30-06-2026 r.
Wymagania szczegółowe	Administracja zdalna w chmurze 1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.

	5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. Ochrona stacji roboczych 31. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 32. Rozwiązanie musi wspierać architekturę ARM64. 33. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 34. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 35. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 36. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 37. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 38. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 39. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 40. Rozwiązanie musi integrować się z Intel Threat Detection Technology. 41. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie

	dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 42. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 43. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 44. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 45. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 38. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 39. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 40. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 41. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

	42. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 43. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. Ochrona serwera 48. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux. 49. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 50. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 51. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 52. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 53. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

	54. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 55. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. Dodatkowe wymagania dla ochrony serwerów Windows: 58. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej . 59. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 60. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 61. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 62. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 63. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 64. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 65. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 66. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe wymagania dla ochrony serwerów Linux: 57. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 58. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 59. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, 60. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. Szyfrowanie 61. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.

	62. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 63. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 64. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. Ochrona urządzeń mobilnych opartych o system Android 65 Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 66 Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 67 Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 68 Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: usunięcie zawartości urządzenia, przywrócenie urządzenie do ustawień fabrycznych, zablokowania urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła. Sandbox w chmurze 67. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 68. Rozwiązanie musi wykorzystywać do działania chmurę producenta. 69. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 68. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 69. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.

	68. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 69. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. 70. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. 1 Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 2 Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. 3 Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. a. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: Czysty, b. Podejrzany, c. Bardzo podejrzany, d. Szkodliwy. 78. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. 79. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. 80. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia. Moduł XDR 109. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 110. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 111. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 112. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 113. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. 114. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. 115. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.

	116. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. 117. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 118. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 119. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 120. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. 121. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. 122. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. 123. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich. 124. Konsola administracyjna musi mieć możliwość tagowania obiektów. 125. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
Ilość	1 szt.

ETAP II

1. MACIERZ DYSKOWA NA POTRZEBY PCPR

Nazwa	

	Minimalne wymagania dla sprzętu
Typ	Zakup macierzy dyskowej zabezpieczającej przed utratą danych na potrzeby PCPR wraz z montażem, konfiguracją i wsparciem serwisowym
Obudowa	System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''. Maksymalna wysokość systemu nie może przekraczać 2U.
Pojemność:	System musi zostać dostarczony w konfiguracji zawierającej minimum: • 8 dysków 1900GB SSD • 6 dysków 1,2TB SAS, o prędkości obrotowej minimum 10 tyś. Obr/min. Wszystkie oferowane dyski muszą być podłączone interfejsem o prędkości co najmniej 12Gb SAS. System musi ponadto wspierać dyski o wielkościach co najmniej: • SSD: od 800GB do 15.3TB • SAS 10k od 900GB do 1800GB • NL-SAS/SATA od 4TB do 18TB System musi mieć możliwość rozbudowy do minimum 180 dysków oraz musi pozwalać na rozbudowę do wyższych modeli bez potrzeby migracji danych (przez rozbudowę do wyższego modelu zamawiający rozumie do modelu macierzy z większą ilością Cache, większą skalowalnością i mocniejszymi procesorami) . Zamawiający dopuszcza rozwiązanie, które nie pozwala na taką rozbudowę w przypadku gdy zostanie zaoferowana macierz skalowalna min. do 500 dysków oraz pamięcią cache min 512GB.
Kontroler	Minimum dwa kontrolery wyposażone w przynajmniej 8GB cache każdy. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash.
Interfejsy	Oferowana macierz musi posiadać minimum • 4 portów 10GbE (uniwersalne wkładki SFP+) • 4 porty SAS 12 Gb/s • 4 porty 1GbE do zarządzania dostępne dla użytkownika oraz 2 porty konsolowe (RJ45) Macierz musi umożliwiać rozbudowę o dodatkowe porty 8 portów 12Gb SAS, FC o prędkości 32Gb lub 25Gb ISCSI. rozbudowa portów musi się odbywać tylko poprzez dołożenie odpowiednich kart rozszerzeń lub wymianę kart, bez konieczności wymiany kontrolerów macierzy.
RAID	Wsparcie dla RAID: 0, 1, 5, 6, 10 Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum 180 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych. Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy. Zamawiający dopuszcza zastosowanie zewnętrznego narzędzia (software, volume manager, SDS) to zbudowania RAID 0.

Obsługiwane protokoły	FC, iSCSI, SAS, Macierz musi mieć możliwość wystawienia zasobów dyskowych poprzez protokoły CIFS, NFS, S3. Zamawiający dopuszcza zastosowanie rozwiązania typu SDS (Software Defined Storage).
Funkcjonalności	Macierz musi posiadać funkcjonalność wykonywania snapshotów minimum 128 per wolumen oraz 512 Snapshotów na macierzy Macierz musi posiadać funkcjonalność klonowania danych. Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie. Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy, na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 128 partycji. Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online volumenów logicznych pomiędzy nimi w zależności od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika. Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID, czyli zmianę sposobu zabezpieczenia grupy dyskowej z jednego poziomu RAID na drugi na tych samych dyskach. Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków oraz z poziomu graficznego interfejsu do zarządzania musi być możliwość sprawdzenia stanu zużycia dysków SSD. Wraz z system musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście: - wydajności i opóźnień na wolumenach - wydajności I/Ops, MB/s - trafności w cache Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji. Zamawiający dopuszcza zaoferowania zewnętrznego oprogramowania do zapewnienia integracji i monitoring w/w aplikacji. Macierz musi zapewniać możliwość szyfrowania danych, realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami. Wraz z macierzą musi zostać dostarczone narzędzie (w formie dedykowanej aplikacji, portalu www lub innej) do monitoringu macierzy w tym przechowywania danych historycznych z min 6 mcy o: - wydajności macierzy - zajętości przestrzeni - błędach/awariach, które wystąpiły na macierzy Narzędzie może pochodzić od innego dostawcy niż producent macierzy. Wszystkie licencje na funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy.

Gwarancja i serwis	Minimum 36 miesięcy serwisu producenta macierzy z czasem dostawy części zamiennych na następny dzień roboczy Dostęp do centrum serwisowego 24/7 Możliwość zgłaszania awarii 24/7 Minimum 36 miesięcy aktualizacji do oprogramowania oraz dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia.
Wdrożenie	Zamawiający wymaga montażu macierzy wraz z pełną aktualizacją systemu operacyjnego hosta /oprogramowania układowego macierzy na dzień wdrożenia. W ramach wdrożenia należy podłączyć macierz za pomocą dedykowanych przewodów. Zezwala się na połączenie direct między macierzą i serwerem bez wykorzystania dedykowanego przełącznika. Wdrożenie musi być zakończone dokumentacją powdrożeniową.
Ilość	1 szt.

2. SERWER Z PRZEZNACZENIEM DO WIRTUALIZACJI SYSTEMÓW NA POTRZEBY PCPR

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zakup serwera z przeznaczeniem do wirtualizacji systemów, obsługą raid wraz z oprogramowaniem do tworzenia wirtualnej infrastruktury i zarządzania nią na potrzeby PCPR, wraz z licencją i wsparciem serwisowym
Obudowa	• Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. • Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów minimum 32 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowane minimum dwa procesory min. 8-rdzeniowe, taktowane min. 2.9GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 175 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. Wydruk z testu należy dołączyć do oferty. Zamawiający dopuszcza wydruk w języku angielskim.
RAM	Minimum 256GB pamięci RDIMM 5600MT/s,

	Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.
Funkcjonalność pamięci RAM	• Demand Scrubing, • Patrol Scrubing, • Permanent Fault Detection
Gniazda PCI	minimum dwa sloty PCIe generacji 5
Interfejsy sieciowe/FC/SAS	• Wbudowane: - min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT - min. 4 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Dyski twarde	Zainstalowane minimum 2 dyski SSD M.2 o pojemności min. 480GB w RAID 1
Wbudowane porty	Minimum 4 x USB z czego nie mniej niż 1x USB 3.0, 2x VGA
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 1100W każdy.
System Operacyjny	Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO, pokrywającego licencyjnie Wszystkie core oferowanych procesorów. Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym minimum dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu,

	II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, III. zdalna dystrybucja oprogramowania na stacje robocze, IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, VI. szyfrowanie plików i folderów,

	VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), VIII.możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, IX. serwis udostępniania stron WWW, X. wsparcie dla protokołu IP w wersji 6 (IPv6), XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0

	• Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ○ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; ○ możliwość podmontowania zdalnych wirtualnych napędów; ○ wirtualną konsolę z dostępem do myszy, klawiatury; ○ wsparcie dla IPv6; ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie; ○ wsparcie dla dynamic DNS; ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish

	○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.

	○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. Oprogramowanie dostarczane jako wirtualny appliance
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub równoważną • Serwer musi posiadać deklaracja CE lub normą równoważną
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Min. 36 m-cy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez linię telefoniczną producenta. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. • Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 lub równowazne na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
Wdrożenie	Zamawiający wymaga montażu fizycznych serwerów wraz z pełną aktualizacją systemu operacyjnego hosta i maszyn wirtualnych/oprogramowania układowego

	serwera na dzień wdrożenia. Wymagane jest zaadresowanie interfejsu niskopoziomowego zarządzania, oraz serwera fizycznego i maszyn wirtualnych które to Wykonawca musi uruchomić na w/w serwerze. Parametry minimalne w/w maszyn wirtualnych zostaną podane na etapie realizacji wdrożenia. W ramach wdrożenia należy podłączyć dostarczane serwery do dostarczanej macierzy za pomocą dedykowanych przewodów. Zezwala się na połączenie direct między macierzą i serwerem bez wykorzystania dedykowanego przełącznika. W ramach wdrożenia należy wykonać testy redundancji sieci SAN za pomocą fizycznego odpięcia każdej ścieżki. Wdrożenie musi być zakończone dokumentacją powdrożeniową opisującą wszelkie istotne w punktu działania klastra rekonfigurację, w tym opis konfiguracji konsoli niskopoziomowego zarządzania serwerem.
Ilość	1 szt.

3. OPROGRAMOWANIE DO BACKUPU NA POTRZEBY PCPR

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Zakup i wdrożenie oprogramowania służącego do backupu i odzyskiwania danych oraz zarządzania danymi w środowiskach wirtualnych i chmurowych dla PCPR z licencją i wsparciem serwisowym dla PCPR
Parametry techniczne	• Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. • Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL (w tym odtwarzanie point-in-time). • Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania. • Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych. • Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.

	• Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. • Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites. • Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska. • Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska. • Oprogramowanie musi wspierać granularne odtwarzanie baz danych z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. • Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego. • Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. • Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. • Testy muszą być przeprowadzone bez interakcji z administratorem. • Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere. • Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. • System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego bez potrzeby korzystania z narzędzi firm trzecich. • System musi umożliwiać monitorowanie środowiska wirtualizacyjnego System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. • System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii. • System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn. • System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz XLS.

	• System musi dawać możliwość podłączenia się do kilku instancji jednocześnie, w celu centralnego monitorowania wielu środowisk. • System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora. • System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów. • System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard). • System musi wspierać wiele instancji jednocześnie bez konieczności instalowania dodatkowych modułów. • System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach • System musi mieć możliwość eksportowania raportów do formatów DOC, XLS, PDF. • Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego. • Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych. • Rozwiązanie musi wspierać co najmniej dystrybucje systemów Linux • Rozwiązanie musi wspierać systemy operacyjne macOS. • Rozwiązanie musi wspierać wykonywanie kopi zapasowych następujących systemów plików: NTFS, ReFS, FAT32, ext2, ext3, ext4, ReiserFS, JFS, XFS, F2FS, Brtfs (dla kernela 3.16 i nowszych), APFS, HFS, HFS+, NILFS2. • Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą). • Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster. • Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów. • Rozwiązanie musi wspierać backup podłączonych dysków USB. • Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym. • Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na: • Lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, • Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, • Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub • NFS,

	• Zcentralizowanym repozytorium danych, • Bezpośrednio na zasobach Chmury. • Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone. • Rozwiązanie musi wspierać kontrolę pasma sieciowego. • Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych. • Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN. • Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft. • Rozwiązanie musi wspierać skrypty wykonywane przed i po wykonaniu zadania oraz przed i po wykonaniu migawki na poziomie wolumenu. • Rozwiązanie musi wspierać technologię BitLocker. • Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania. • Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowejRozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych. • Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL poprzez bezpośrednie uruchomienie ich z pliku backupu. • Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych • Rozwiązanie musi wspierać szyfrowanie. • Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne. • Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego. • Rozwiązanie musi wspierać tworzenie wielu zadań backupowych. Powyższa funkcjonalność ma działać w środowisku wirtualnym i/lub fizycznym. Wymagane jest dostarczenie licencji wieczystych dla zabezpieczenia minimum 5 sztuk wirtualnych i/lub fizycznych serwerów oraz 25 stacji roboczychWraz z oprogramowanie wymagane jest dostarczenie wsparcia producenta oprogramowania do 30-06-2026 r.
Wdrożenie	Instalacja urządzenia i oprogramowania wykonana przez certyfikowanych pracowników Wykonawcy w zakresie wdrażanego rozwiązania, instalacja i konfiguracja urządzenia, w tym montaż w szafach RACK, podłączenie zasilania, aktualizacja oprogramowania układowego i jego komponentów do rekomendowanych przez producenta wersji, konfiguracja uprawnień użytkowników,

	podłączenie magazynów danych z urządzenia logicznego do dostarczonego oprogramowania do backupu, instalacja modułów oprogramowania do backupu, zaprojektowanie i wdrożenie polityki tworzenia kopii zapasowych z wykorzystaniem dostarczonego oprogramowania do backupu, przeprowadzenie testów akceptacyjnych poprawności działanie operacji, backupu i odzyskiwania danych. Przygotowanie dokumentacji powykonawczej, zawierającej minimum: schematy połączeń pomiędzy systemem backupowym, a innymi urządzeniami podłączonymi do dostarczanego systemu, adresację systemów, konfigurację modułów oprogramowania
Ilość	1 szt.

4. PRZEŁĄCZNIK SIECIOWY WIELOWARSTWOWY L3 NA POTRZEBY PCPR

Nazwa	**Minimalne wymagania dla sprzętu**
Typ	Zakup przełącznika sieciowego wielowarstwowego L3, zarządzalnego wraz z konfiguracją, instruktarzem stanowiskowym i wsparciem serwisowym na potrzeby PCPR
Parametry techniczne	• Typ przełącznika: Zarządzany • Przełącznik wielowarstwowy L3 • Porty: Minimum 48 x 10/100/1000 (PoE+) + minimum 4 x Gigabit SFP • Liczba portów USB 2.0: minimum 3 • Zasilanie przez Ethernet: PoE+ • Zasilanie na port:minimum 30W • Budżet PoE: minimum 740W • Przepustowość zagregowana: minimum 80 Gbps • Zdolność przełączania: minimum 100 Gbps • Szybkość przekierowywania: minimum 150 Mp/s • Sieci wirtualne: minimum 1 • Trasy IPv4: minimum 11000 • Wpisy w tabeli routingu IPv4: minimum 3000 • Wpisy w tabeli routingu IPv6: minimum 1500 • Skala multicast: minimum 1000 • Wpisy skali ACL: minimum 1500 • Wpisy FNF: minimum 16000 • Obsługuje VLANs: minimum 1024 • Wirtualny interfejs: minimum 512 • Kolejki priorytetowe na port: minimum 8 • Wielkość tabeli adresów: minimum 16000 wpisów • Obsługiwane ramki Jumbo: minimum 9198 bajtów • Protokół routingu: OSPF, RIP-1, RIP-2, EIGRP, VRRP, PIM-SM, EIGRP for IPv6, PIM-SSM, policy-based routing (PBR), RIPng, MSTP

	• Protokół zdalnego zarządzania: SNMP 1, RMON 1, RMON 2, SNMP 3, SNMP 2c, CLI, NETCONF, RESTCONF • Standardy komunikacyjne: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3at, IEEE 802.3bz, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z • Pojemność pamięci wewnętrznej minimum 2048 MB • Wielkość pamięci flash minimum 4096 MB • Zakres temperatur eksploatacji: -5 - 45°C • Zakres temperatur przechowywania: -40 - 70°C • Zakres wilgotności względnej: 5 - 90% • Dopuszczalna wysokość podczas eksploatacji (n.p.m.): 0 - 3000 m
Gwarancja	Minimum 12 miesięcy producenta
Wdrożenie i instruktaż stanowiskowy	W ramach wdrożenia wymagana jest instalacja urządzenia wykonana przez certyfikowanych pracowników Wykonawcy w zakresie wdrażanego rozwiązania, instalacja i konfiguracja urządzenia, w tym montaż w szafach RACK, podłączenie zasilania, aktualizacja oprogramowania układowego i jego komponentów do rekomendowanych przez producenta wersji. Przygotowanie dokumentacji powykonawczej.
Ilość	1 szt.

ETAP III

1. PRZEŁĄCZNIKI SIECIOWE L3 I AKCESORIA NA POTRZEBY STAROSTWA POWIATOWEGO

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zakup 2 szt. przełączników sieciowych L3, wkładek SFP, - moduły wraz z montażem, konfiguracją w środowisku sieciowym, instruktażem stanowiskowym oraz wsparciem serwisowym, na potrzeby Starostwa Powiatowego
Dane techniczne i funkcjonalne urządzenia	Przełącznik typu standalone wyposażony w minimum 24 porty 1/10/25 Gigabit Ethernet SFP/SFP+/SFP28 oraz minimum 4 porty uplink 40/100 Gigabit Ethernet QSFP Porty SFP/SFP+/SFP28 muszą umożliwiać zastosowanie następujących wkładek interfejsowych: • Gigabit Ethernet 1000Base-T, • Gigabit Ethernet 1000Base-SX, • Gigabit Ethernet 1000Base-LX/LH, • Gigabit Ethernet 1000Base-EX, • Gigabit Ethernet 1000Base-ZX, • Gigabit Ethernet 1000Base-BX-D/U, • 10Gigabit Ethernet 10GBase-SR, • 10Gigabit Ethernet 10GBase-LR, • 10Gigabit Ethernet 10GBase-ER, • 10Gigabit Ethernet 10GBase-ZR, • 10Gigabit Ethernet 10GBase-BX-D/U,

	• 10Gigabit Ethernet typu twinax (SFP+ - SFP+), • 25Gigabit Ethernet 25GBASE-SR, • 25Gigabit Ethernet typu twinax (SFP28 – SFP28), • 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF), • 10/25Gigabit Ethernet 10/25GBASE-LR (SMF); Porty QSFP umożliwiają zastosowanie następujących modułów interfejsowych: Dla transmisji 40Gb/s: · 40G-SR4, · 40G-LR4, · 40G-ER4, · 40G-SR-BD, · 40G-CSR, · 40G-CSR4, · 40G-LR4-Lite (zasięg 2 km dla światłowodu SMF G.652), · adapter 40G QSFP->10G SFP+, • 40Gigabit Ethernet typu twinax (QSFP - QSFP); Dla transmisji 100Gb/s: • 100GBASE-SR4, • 100GBASE-LR4, • 100Gigabit Ethernet typu twinax (QSFP - QSFP); Urządzenie powinno być wyposażone w wymienne moduły wentylatorów,
Wydajność	Urządzenie powinno posiadać minimum 32MB bufor pamięci, Minimum 16GB pamięci DRAM i minimum 16GB pamięci flash, Przepustowość przełącznika (switching capacity) minimum 1.6 Tbps, Prędkość przesyłania (forwarding rate) minimum 1 miliard pps (1Bpps), Obsługa minimum: • 1000 aktywnych sieci VLAN, • 80 000 adresów MAC, • 212 000 tras IPv4, • 212 000 tras IPv6, • Ilość wpisów w listach kontroli dostępu Security ACL – 27 000, • ilość wpisów w listach kontroli dostępu QoS ACL – 16 000, • 1000 interfejsów SVI L3, • Jumbo frame 9198B, • 128 połączeń zagregowanych typu „port channel”, • 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP;
Oprogramowanie/funkcjonalność	Obsługa protokołu NTP, Obsługa IGMPv1/2/3, Obsługa standardu IEEE 802.1ae (MACSec) szyfrowanie ruchu z kluczami o długości 256-bitów dla wszystkich interfejsów przełącznika. Wsparcie dla uruchomienia MACsec na portach tworzących połączenia zaagregowane L2 i L3, System operacyjny przełącznika umożliwia wgrywanie poprawek bez konieczności restartowania platformy, System operacyjny przełącznika jest konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelów danych YANG (RFC 6020) oraz

	umożliwia eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów, Wsparcie dla protokołu RESTCONF, Możliwość uruchamiania zdefiniowanych w Pythonie skryptów w chwili zaistnienia określonego zdarzenia, Przełącznik realizuje następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: • IEEE 802.1w Rapid Spanning Tree, • Per-VLAN Rapid Spanning Tree (PVRST+), • IEEE 802.1s Multi-Instance Spanning Tree, • Obsługa 1000 instancji protokołu STP; Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED, Realizacja funkcji 802.1Q tunneling (QinQ), Funkcja serwera DHCP, Obsługa minimum 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level), Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+, Obsługa list kontroli dostępu (ACL) następujących typów: · Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, · VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika, · Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN, · Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia); Przełącznik realizuje następujące mechanizmy związane z zapewnieniem, jakości usług w sieci: • Minimum 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, • Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek, • Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), • Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, • Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting), • Kontrola sztormów dla ruchu broadcast/multicast/unicast, • Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

	Przełącznik posiada wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing), Realizacja funkcji Private VLAN zarówno na portach dostępowych oraz portach trunk (obsługa wielu sieci primary VLAN na jednym porcie trunk oraz wielu sieci secondary vlan na jednym porcie trunk), Urządzenie realizuje routing statyczny i dynamiczny dla IPv4 i IPv6 w zakresie: • Routing statyczny dla IPv4 i IPv6, • Routing dynamiczny dla IPv4: BGP, ISIS, • Routing dynamiczny dla IPv4: OSPF, EIGRP (rfc7868) wraz z obsługą mechanizmu IP FRR (Fast Reroute) Loop Free Alternate (LFA), • Routing dynamiczny dla IPv6: OSPFv3, • Funkcjonalności Policy-based routing, • multicast routing (PIM-SM, PIM-SSM) , • Obsługa protokołu redundancji bramy (VRRP) z obsługą 255 grup, • Obsługa 200 tuneli GRE (Generic Routing Encapsulation), • Obsługa 1000 wirtualnych instancji routingu (VRF), Obsługa protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa minimum 100 sesji BFD, Realizacja funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 3000 translacji, Urządzenie realizuje protokołu LISP zgodnie z RFC 6830, Urządzenie umożliwia enkapsulację ruchu przy pomocy VXLAN'ów, Wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności węzłów leaf / spine / border, Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia, Urządzenie jest przygotowane sprzętowo do łączenia w klaster z drugim takim samym urządzeniem (tzw. wirtualne stakowanie). Urządzenia w klastrze będą zachowywać się jak jedno urządzenie w punktu widzenia protokołów L2 i L3, Klastrowanie wspiera funkcję eliminacji przesyłania ruchu BUM (Broadcast, unknown-unicast and multicast traffic) poprzez połączenie realizujące klaster pomiędzy przełącznikami, Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN, Możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN), Funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: dhcp, dns, ftp, http, icmp-echo, icmp-jitter, tcp-connect, udp-echo, udp-jitter,

	Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego, Wbudowany analizator pakietów, Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników: • Statycznie w oparciu o port, do którego podłączona jest stacja, • Statycznie w oparciu o VLAN, w którym pracuje stacja, • Statycznie w oparciu o adres IP stacji, • Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X; Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu, Propagacja informacji o przypisaniu stacji danego znacznika bezpieczeństwa (secure tag) bezpośrednio w ramce Ethernet (metoda in-line) lub za pomocą mechanizmu out-of-band, który przekazuje do urządzeń dokonujących wymuszenia polityki mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa, Urządzenie umożliwia uruchamianie dodatkowych aplikacji w kontenerach Docker, Urządzenie może zostać wyposażone w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci dysku M2 SATA o pojemności minimum 240/480/960GB.
Funkcjonalności z zakresu MPLS	Urządzenie musi realizować następujące funkcjonalności z zakresu MPLS: •L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 1000 połączeń wirtualnych VC, •L2VPN - Virtual Private LAN Services (VPLS) - obsługa minimum 1000 wirtualnych instancji (VFI), minimum 32 sąsiadów w ramach jednej instancji, •L3 VPN - MPLS Virtual Private Network (VPN), •Multicast VPN (MVPN); •Inter AS Option A i B, •EoMPLS wraz z obsługa MACSec (MACsec over EoMPLS), •MPLS over GRE,
Zarządzanie i konfiguracja	Urządzenie realizuje sprzętowo tworzenie statystyk ruchu w oparciu o pełen NetFlow (bez próbkowania), wielkość tablicy monitorowanych strumieni minimum 98 000, Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych, Urządzenie powinno posiadać dedykowany port Ethernet do zarządzania out-of-band,

	Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA, Urządzenie powinno posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB, Urządzenie powinno być wyposażone w port konsoli USB, Urządzenie powinno umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie, Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6, Przełącznik powinno posiadać wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą i identyfikacji konkretnego urządzenia, Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych, Funkcja programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące
Obudowa	Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU.
Wyposażenie urządzenia dodatkowe	Przełącznik powinno być wyposażone w następujące moduły interfejsowe SFP / SFP+ pochodzące z oferty producenta przełącznika minimum: • 10Gigabit Ethernet 10GBase-LR, - minimum 2 sztuki Przełącznik powinno być wyposazone w następujące moduły QSFP pochodzące z oferty producenta przełącznika: · 100GBASE-LR4, - minimum 4 sztuki
Gwarancja i wsparcie	Urządzenie powinno być wyposażone w licencje subskrypcyjną na wymagane funkcjonalności do 30-06-2026 r. Zamawiający wymaga dostarczenia urządzeń wraz ze wsparciem do 30-06-2026 r.
Ilość	1 kpl.

1 URZĄDZENIE KLASY UTM NA POTRZEBY STAROSTWA POWIATOWEGO

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zakup i wdrożenie urządzenia UTM o wysokiej przepustowości na potrzeby Starostwa Powiatowego
Wymagania ogólne	Zamawiający jest obecnie w posiadaniu urządzenia FortiGate-200F o numerze seryjnym FG200FT920904913. Oferowane rozwiązanie musi mieć możliwość utworzenia klastra z posiadanym przez Zamawiającego urządzeniem.. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

	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 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Wymagania równoważności	
Redundancja, monitoring i wykrywanie awarii	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. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie:	System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 18 portami Gigabit Ethernet RJ-45. 8 gniazdami SFP 1 Gbps. 4 gniazdami SFP+ 10 Gbps. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. System jest wyposażony w zasilanie 2xAC.
Parametry wydajnościowe:	W zakresie Firewall'a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz minimum 280 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 27 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 13 Gbps. Wydajność szyfrowania IPSec VPN nie mniej niż 12 Gbps. 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 5 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4 Gbps.
Funkcje Systemu Bezpieczeństwa:	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

	Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. Kontrola Aplikacji. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. Ochrona przed malware. Ochrona przed atakami - Intrusion Prevention System. Kontrola stron WWW. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. Zarządzanie pasmem (QoS, Traffic shaping). Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 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. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 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).
Polityki, Firewall	Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: Translację jeden do jeden oraz jeden do wielu. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 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.
Połączenia VPN	System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: Wsparcie dla IKE v1 oraz v2. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). Obsługa protokołu Diffie-Hellman grup 19, 20. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.

	Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. Mechanizm „Split tunneling" dla połączeń Client-to-Site. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: 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. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. 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.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: Routingu statycznego. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. BFD (Bidirectional Forwarding Detection). Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. System daje możliwość określania pasma dla poszczególnych aplikacji. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware	Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 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. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 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. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

	Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 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).
Kontrola WWW	Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 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. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 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. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie	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. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	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. 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. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. Możliwość włączenia logowania per reguła w polityce firewall. System zapewnia możliwość logowania do serwera SYSLOG. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Certyfikaty	Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje: ICSA lub EAL4 lub równoważne dla funkcji Firewall.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres do 30-06-2026 r.

	System musi być objęty serwisem gwarancyjnym producenta przez okres do 30-06-2026 r., 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.
Wdrożenie	Montaż w szafie i utworzenie klastra z posiadanym przez Zamawiającego urządzeniem.
Ilość	1 szt.

3. BIBLIOTEKA TAŚMOWA LTO 9 NA POTRZEBY STAROSTWA POWIATOWEGO

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zakup i wdrożenie biblioteki taśmowej LTO 9 wraz z tasiemkami i serwerem sterującym oraz licencją i wsparciem serwisowym na potrzeby Starostwa Powiatowego
Ogólne	Przedmiotem zamówienia jest dostarczenie urządzenia taśmowego umożliwiającego przechowywanie danych na nośnikach taśmowych typu LTO.
Obudowa	Urządzenie nie może przekraczać rozmiaru 3U w podstawowej konfiguracji. Po rozbudowie pomiędzy poszczególnymi modułami biblioteki musi być możliwość automatycznego przemieszczania nośników z wykorzystaniem jednego robota, który musi mieć dostęp do wszystkich kieszeni na nośniki. Biblioteka musi być wyposażona w zestaw umożliwiający jej zamontowanie w szafie Rack 19”.
Napędy i obsługiwane nośniki	Biblioteka musi być wyposażona minimum dwa napędy w technologii LTO9. Musi umożliwiać wymianę napędów bez przerwania pracy biblioteki. Minimalna pojemność taśmy bez kompresji 12TB. Każdy z napędów taśmowych musi posiadać interfejs SAS o prędkości minimum 12Gb/s.
Kieszenie na nośniki (sloty)	Biblioteka musi mieć minimum 50 kieszeni na nośniki, jeśli ich obsługa wymaga dodatkowych licencji wymagane jest dostarczenie takiej licencji. Biblioteka musi mieć możliwość zdefiniowania co najmniej 1 kieszeni typu „mail slot”.
Rozbudowa	Ze względu na przyszłościowe zastosowanie wymaga się, aby biblioteka miała możliwość rozbudowy do 24 napędów taśmowych i była w stanie obsłużyć co najmniej 400 slotów wspólnie zarządzanych przez jeden moduł kontrolny.
Zarządzanie	Biblioteka musi być wyposażona w moduł zdalnego zarządzania. Biblioteka musi udostępniać funkcję monitorowania napędów. Biblioteka powinna mieć również możliwość zdalnego monitorowania urządzenia i wychwytywania błędów bezpośrednio przez inżynierów producenta za pomocą odpowiedniego oprogramowania.
Pozostałe wymagania	Biblioteka musi posiadać czytnik kodów kreskowych do identyfikacji taśm. Biblioteka musi zostać dostarczona z redundantnym zasilaniem.

	Biblioteka musi mieć w przyszłości możliwość wsparcia technologii szyfrowania danych kluczem o sile AES-256. Biblioteka powinna być wykonana w technologii umożliwiającej sprzętowy podział na mniejsze biblioteki „logiczne", a następnie podłączanie do różnych serwerów, korzystając z różnego oprogramowania do wykonywania kopii zapasowych i archiwizacji. Biblioteka powinna posiadać możliwość rozbudowy o mechanizm fizycznej blokady przed możliwością załadowania taśmy przez robot do napędu. Fizyczna blokada powinna być możliwa do uruchomienia przez operatora. Blokada powinna umożliwiać odczytanie kodu kreskowego znajdującego się na taśmie. Blokada musi być natywnym rozwiązaniem wspieranym przez producenta biblioteki.
Serwis	Biblioteka powinna być objęta minimum 3 letnią gwarancją i wsparciem producenta biblioteki z możliwością zgłaszania awarii w trybie 5x9 z czasem dostawy części w trybie następnego dnia roboczego z usługą wymiany części na miejscu. W okresie serwisu zamawiający musi mieć dostęp do zdalnej pomocy technicznej, poprawek i nowych wersji oprogramowania i sterowników oferowanej biblioteki. Dodatkowo minimum 10 kompatybilnych tasiemek LTO9.
Wymaganie dla serwera sterującego	
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 3.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa z możliwością wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowany minimum jeden procesor serwerowy minimum 8-rdzeniowy, min. 2.8 GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 19 100 pkt w teście Average CPU Mark dostępnym na stronie https://www.cpubenchmark.net/.
RAM	Minimum 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
Gniazda PCI	- minimum dwa sloty PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. - 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT - 2 interfejsy sieciowe 10/25 Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)

	- 4 interfejsy SAS HBA 12Gbps
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane minimum 3 dyski serwerowe o pojemności min. 8TB wymieniane bez wyłączenia systemu, zorganizowane w RAID5 Zainstalowane minimum dwa dyski M.2 SATA o pojemności min. 240GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w minimum 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
Wbudowane porty	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug minimum 1100W o klasie sprawności Titanium
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;

	• możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub równoważną. Serwer musi posiadać deklaracja CE lub równoważne.
Warunki gwarancji	Min. 36 miesięcygwarancji realizowanej przez Producenta urządzenia lub jego Autoryzowany Serwis. Gwarancja świadczona w miejscu instalacji sprzętu z czasem podjęcia naprawy na następny dzień roboczy. W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego – dokument potwierdzający spełnienie tego warunku załączyć do oferty. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy /

	producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 lub równoważne na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokument potwierdzający spełnienie tego warunku załączyć do oferty.
Dokumentacja użytkownika	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Wdrożenie	Montaż w szafie i uruchomienie biblioteki wraz z połączeniem do serwera sterującego.
Ilość	1 kpl.