Załącznik nr 9B do SWZ

Szczegółowy opis przedmiotu zamówienia (OPZ)

Przedmiotem zamówienia jest dostawa sprzętu i oprogramowania zwanych dalej: „sprzętem" lub „produktem" w ramach zadania „Cyberbezpieczny Samorząd w Gminie Świebodzice". Zamówienie jest zgodnie z wnioskiem o dofinansowanie i obejmuje zgodnie z poniższą specyfikacją techniczną :

1. System Bezpieczeństwa – 1 sztuka

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 powinien zapewnić pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System musi umożliwić 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 5 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 musi zapewnić 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 musi umożliwić agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. 5. System ma pracować w postaci redundantnego klastra (minimum dwa fizyczne urządzenia lub rozwiązanie równoważne)
Interfejsy, zasilanie	1. System realizujący funkcję Firewall musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów: • 8 portami Gigabit Ethernet RJ-45. • 2 gniazdami SFP+ 10 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 3. System Firewall musi pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 25 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 4 Gbps. 6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.5 Gbps.
Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Muszą 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. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. 13. Rozwiązanie musi posiadać 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 musi uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi realizować 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 musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Musi umożliwiać wykorzystanie w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. 5. Polityka firewall musi umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Musi zapewnić ustawienie przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.

Połączenia VPN	1. System musi umożliwiać 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. Producent rozwiązania musi posiadać w ofercie bezpłatne 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 musi zapewniać obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	1. System musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN musi wspierać zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System musi dawać możliwość określania pasma dla poszczególnych aplikacji. 3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona antywirusowa i ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych musi istnieć możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który System Bezpieczeństwa może poświęcić na dekompresję archiwum. 4. System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System musi dysponować 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 musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. 8. System musi zapewnić możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 9. System musi zapewnić 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 musi chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków musi zawierać minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewnić wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. System musi posiadać mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. System musi wykrywać i blokować komunikację C&C do sieci botnet. 8. System musi zapewnić możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji musi zawierać minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. 6. Musi Istnieć możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System musi możliwiać 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 musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW musza być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorie stron zabronionych prawem np.: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW musi umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW musi dawać możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. System musi posiadać funkcję Safe Search – przeciwdziałającą pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System musi pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać 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. 2. System musi dawać możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 3. System musi umożliwiać 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. System musi zapewniać 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 ma być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Musi mieć możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System musi dawać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. System musi posiadać możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu. 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować 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 musi zapewniać 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 musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. System musi zapewniać możliwość włączenia logowania per reguła w polityce firewall. 5. System musi zapewniać możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów musi być możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu musza być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.

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 24 miesięcy.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent musi zapewniać dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Inne	W ramach niniejszego postępowania wymaga się przeniesienia konfiguracji z posiadanego i użytkowanego przez Zamawiającego urządzenia firmy Fortinet model FG-201E i zaimplementowanie konfiguracji w zaoferowanym Systemie Bezpieczeństwa.

2. Przełącznik sieciowy 52 portowy - 7 sztuk

W ramach postępowania wymaga się dostarczenia elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaga się dostarczenia przełączników oraz innych elementów funkcjonalnych, współpracujących z oferowanym Systemem Bezpieczeństwa, o następujących parametrach:

Parametry fizyczne platformy	• Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. • Zasilanie AC 230V. • Budżet mocy dla portów PoE min.: 370 W. • Maksymalny pobór mocy bez budżetu dla PoE: 110 W. • Minimalny zakres temperatury pracy: 0-40°C.
Interfejsy sieciowe	Wymaga się, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: a) min. 48 porty GE RJ-45; w tym porty PoE w ilości co najmniej: 24, zgodne ze standardem: 802.3af oraz 802.3at; b) min. 4 porty 10 GE SFP+.
Zarządzanie	• Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). • Wsparcie dla SNMP w wersjach 1-3 • Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. • Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. • Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. • Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). • Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. • Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. • Automatycznie wykonywane rewizje konfiguracji.
Parametry wydajnościowe	• Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. • Tablica adresów MAC o pojemności co najmniej 32k wpisów. • Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
Wymagane funkcje	• Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. • Obsługa Jumbo Frames. • Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). • Agregacja portów zgodna ze standardem 802.3ad. • Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. • Obsługa routingu statycznego. • Port-mirroring. • Uwierzytelnianie 802.1x na poziomie portu. • Uwierzytelnianie 802.1x w oparciu o adres MAC. • W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). • W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. • W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. • Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	1. Przełącznik musi wspierać tryb pracy, w którym jest zarządzany przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: • centralne zarządzanie konfiguracją urządzenia; • aktualizacja oprogramowania realizowana z systemu centralnego zarządzania; • centralne zarządzanie sieciami VLAN; • blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u; • rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.; • przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej; • integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego; • automatyczna detekcja i rekomendacje konfiguracji; • przesyłanie logów na zewnętrzny serwer syslog; • funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników; • obsługa białych i czarnych list adresów MAC; • wykrywanie aplikacji komunikujących się w sieci; 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania konieczne jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. • System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

3. Przełącznik sieciowy 10 portowy - 10 sztuk

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym Systemem Bezpieczeństwa, o następujących parametrach:

Parametry fizyczne	• Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. • Zasilanie AC 230V. • Budżet mocy dla portów PoE min.: 65 W. • Maksymalny pobór mocy bez budżetu dla PoE: 10 W. • Minimalny zakres temperatury pracy: 0-40°C.
Interfejsy sieciowe	Wymaga się aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: a) min. 8 portów GE RJ-45; w tym porty PoE w ilości co najmniej: 8, zgodne ze standardem: 802.3af oraz 802.3at; b) min. 2 porty GE, SFP.
Zarządzanie	• Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. • Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). • Wsparcie dla SNMP w wersjach 1-3 • Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. • Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. • Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. • Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). • Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. • Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. • Automatycznie wykonywane rewizje konfiguracji.
Parametry wydajnościowe	• Przepustowość urządzenia - min. 20 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 30 Mpps. • Tablica adresów MAC o pojemności co najmniej 8 k wpisów. • Opóźnienie wprowadzane przez przełącznik - poniżej 5 mikrosekund.
Wymagane funkcje	• Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. • Obsługa Jumbo Frames. • Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). • Agregacja portów zgodna ze standardem 802.3ad. • Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. • Obsługa routingu statycznego. • Port-mirroring. • Uwierzytelnianie 802.1x na poziomie portu. • Uwierzytelnianie 802.1x w oparciu o adres MAC. • W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). • W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. • W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	**1.** Przełącznik musi wspierać tryb pracy, w którym jest zarządzany przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler, tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: • centralne zarządzanie konfiguracją urządzenia; • aktualizacja oprogramowania realizowana z systemu centralnego zarządzania; • centralne zarządzanie sieciami VLAN; • blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u; • rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.; • przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej; • integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego; • automatyczna detekcja i rekomendacje konfiguracji; • przesyłanie logów na zewnętrzny serwer syslog; • funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników; • obsługa białych i czarnych list adresów MAC; • wykrywanie aplikacji komunikujących się w sieci. **2.** Musi być możliwe redundantne połączenie z elementami zarządzającymi. **3.** W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. • System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

4. Wewnętrzy punkt dostępowy - 3 sztuki

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
    a. Temperatura -20 – 45°C;
    b. Wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
3. Urządzenie musi być wyposażone w dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
    a. 2.4 GHz 802.11b/g/n,
    b. 5 GHz 802.11a/n/ac.
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
5. Urządzenie musi być wyposażone w moduł BLE.
6. Urządzenie musi być wyposażone w jeden interfejs 10/100/1000 Base-TX.
7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3af lub zewnętrzny zasilacz.
8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
    a. Tunnel,
    b. Bridge,
    c. Mesh.
9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
11. Funkcja zarządzania poprzez dedykowany kontroler lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie punktami dostępowymi.
12. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    a. MIMO – 2x2,
    b. maksymalna przepustowość dla poszczególnych modułów radiowych:
        i. 400 Mbps dla pasma 2.4GHz;
        ii. 867 Mbps dla pasma 5GHz;
    c. wymagana moc nadawania:
        i. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
        ii. min. 24 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
    d. wsparcie dla 802.11n 20/40Mhz HT;

e. wsparcie dla kanałów 80MHz;

f. anteny – 4 wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz;

g. nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy;

h. maksymalna deklarowana liczba klientów per moduł radiowy:

   i. 512 dla pasma 2.4GHz;
   ii. 512 dla pasma 5GHz.

13. Funkcje dodatkowe:

    a. 802.11ac MU-MIMO Wave 2;

    b. Transmit Beam Forming (TxBF);

    c. Low-Density Parity Check (LDPC) Encoding;

    d. Maximum Likelihood Demodulation (MLD);

    e. Maximum Ratio Combining (MRC);

    f. A-MPDU and A-MSDU Packet Aggregation;

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

5. Zewnętrzny punk dostępowy - 1 sztuka

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na słupie lub ścianie na zewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
    a. Temperatura -40 – 60°C;
    b. Wilgotność 10–90%.
2. Obudowa musi spełniać normę IP67.
3. Urządzenie musi być dostarczone z elementami mocującymi oraz zasilaczem.
4. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington.
5. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
    a. 2.4 GHz 802.11b/g/n;
    b. 5 GHz 802.11a/n/ac/ax;
    c. Skaner 2.4GHz i 5GHz.
6. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
7. Urządzenie musi być wyposażone w moduł BLE.
8. Liczba interfejsów:
   Co najmniej 2 w standardzie 10/100/1000 Base-TX
9. Urządzenie powinno być zasilane poprzez interfejs ETH zgodnie ze standardem 802.3at oraz być zgodne ze standardem 802.3az.
10. Urządzenie musi posiadać wbudowane zabezpieczenie przeciwprzepięciowe.
11. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
    a. Tunnel;
    b. Bridge;
    c. Mesh.
12. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
13. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3 PSK, WPA3-Enterprise, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
14. Funkcja zarządzania poprzez dedykowany kontroler lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie punktami dostępowymi.
15. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    a. MIMO – 2x2;
    b. maksymalna przepustowość dla poszczególnych modułów radiowych:
        i. 2.4GHz 574 Mbps;
        ii. 5GHz 1200 Mbps;
    c. wymagana moc nadawania:
        i. min. 27 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
        ii. min. 25 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
    d. wsparcie dla 802.11n 20/40Mhz HT;
    e. wsparcie dla kanału 80 MHz;
    f. anteny – wbudowane anteny o zysku min. 10dBi;
    g. nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy;
    h. maksymalna deklarowana liczba klientów dla poszczególnych modułów radiowych:
        i. 512 dla pasma 2.4GHz;
        ii. 512 dla pasma 5GHz.
16. Funkcje dodatkowe:
    a. OFDMA UL i DL;

b. Spatial Reuse (BSS Coloring);
c. UL-MU-MIMO 802.11ax;
d. DL-MU-MIMO;
e. Enhanced Target Wake Time (TWT).

17. Punkt dostępowy musi być certyfikowanym urządzeniem WiFi Alliance oraz posiadać certyfikację DFS.

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

6. Moduł światłowodowy kompatybilny z przełącznikiem pkt. 2 i pkt.3 - 14 sztuk

6.1.Moduł światłowodowy SFP+ 10GBASE-SR - 10 sztuk

Standard protokołu	10GBase-SR
IEEE Standard	802.3ae
Typ modułu	SFP+
Prędkość danych (Ethernet)	10 Gbps
Typ złącza	Duplex LC
Rodzaj światłowodu	Multi-mode
Długość fali	850nm
Zasięg	300m

Moduł światłowodowy SFP+ 10GBASE-LR - 4 sztuki

Standard protokołu	10GBase-LR
IEEE Standard	802.3ae
Typ modułu	SFP+
Prędkość danych (Ethernet)	10 Gbps
Typ złącza	Duplex LC
Rodzaj światłowodu	Single-mode
Długość fali	1310nm
Zasięg	10km

7. Centralny system logowania, raportowania i korelacji - 1 sztuka

Wymagania Ogólne	W ramach postępowania obejmującego dostarczenie Systemu Bezpieczeństwa, przełączników oraz punktów dostępowych wymaga się dostarczenia centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury. 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 na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).
Interfejsy, Dysk	System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności minimum 3 TB.
Parametry wydajnościowe	1. System musi być w stanie przyjmować minimum 5 GB logów na dzień. 2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.
W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:	
Logowanie	1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. 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: a. listę najczęściej wykrywanych ataków; b. listę najbardziej aktywnych użytkowników; c. listę najczęściej wykorzystywanych aplikacji; d. listę najczęściej odwiedzanych stron www; e. listę krajów, do których nawiązywane są połączenia; f. listę najczęściej wykorzystywanych polityk Firewall; g. informacje o realizowanych połączeniach IPSec. 4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 5. 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. 6. 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: 1. generowanie raportów co najmniej w formatach: PDF, CSV; 2. predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników; 3. funkcję definiowania własnych raportów; 4. możliwość „spolszczenia” raportów, w przypadku, kiedy dostępne będą raporty w języku obcym; 5. 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.
Zarządzanie	1. 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. 2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. 3. 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	1. 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 przez okres 24 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

8. Serwer (host klastra wirtualizacyjnego) - 1 sztuka

Zaoferowany serwer będzie częścią posiadanego przez Zamawiającego klastra wirtualizacyjnego opartego na dwóch serwerach HPE DL360 G10, które są monitorowane za pomocą oprogramowania HPE OneView. W przypadku zaoferowania serwera, który nie będzie kompatybilny z oprogramowaniem HPE OneView wymaga się dostarczenia alternatywnego rozwiązania do monitorowania wszystkich serwerów klastra o funkcjonalnościach nie gorszych niż te, które są dostępne w oprogramowaniu HPE OneView Standard, za pomocą których będzie możliwa inwentaryzacja, monitorowanie stanu, przesyłanie alertów oraz raportów dotyczących wszystkich hostów klastra.

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 1U RACK 19 cali wraz z szynami montażowymi umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia. Serwer z możliwością wyposażenia w zdejmowany panel przedni z zamkiem chroniącym przed nieuprawionym dostępem do dysków oraz możliwością dołożenia czujnika otwarcia obudowy współpracującego z BIOS/UEFI.
Procesor	Minimum (min.) dwunastordzeniowy, x86 - 64 bity, pracujący z częstotliwością bazową minimum 2.4GHz i osiągające w testach SPECrate2017_int_base wynik nie gorszy niż 241 punktów, dla testu oferowanego modelu serwera z 2 procesorami. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org Płyta główna wspierająca możliwość zastosowania minimum dwóch procesorów od 8 do 64 rdzeni, mocy do min. 385W i taktowaniu CPU do min. 3.7GHz.
Liczba procesorów	Min. 1 procesor
Pamięć operacyjna	Min. 256GB RDIMM DDR5 5600 MT/s w modułach pamięci o pojemności min. 32GB każdy Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB.
Sloty rozszerzeń	Min. 2 aktywne gniazda PCI-Express generacji 5, x16 (szybkość slotu – bus width). Możliwość dołożenia trzeciego gniazda PCI-Express generacji 5, x16 (szybkość slotu – bus width). Dwa sloty OCP 3.0 możliwe do obsadzenia poprzez kontrolery sprzętowe dla dysków lub karty sieciowe w dowolnej konfiguracji.
Dysk twardy	Serwer bez klatkowy z możliwością rozbudowy/rekonfiguracji w przyszłości serwera do 10 dysków typu Hot Swap, SAS/SATA/SSD/NVMe, 2,5” montowane z przodu obudowy. W przypadku braku opcji rozbudowy/rekonfiguracji o dodatkowe zatoki dyskowe, serwer standardowo wyposażony w minimum 10 zatok dyskowych SFF gotowych do instalacji dysków SAS/SATA/SSD/NVMe 2,5”typu Hot Swap. Zainstalowane min. 2szt. dysków SSD NVMe 480GB nie zajmujące wnęk na dyski twarde pracujące w konfiguracji ze sprzętowym RAID 1.

Kontroler	Serwer wyposażony w kontroler software dla dysków SATA, obsługujący poziomy: RAID 0, 1, 5, 10. Możliwość zastosowania/wymiany kontrolera na kontroler sprzętowy wyposażony w min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę napędów dyskowych SSD/SATA/SAS/NVMe. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie.
Interfejsy sieciowe	Jedna, czteroportowa karta 1Gb BASE-T nie zajmująca gniazd opisanych w sekcji „słoty rozszerzeń”. Dwie, jednoportowe karty 32Gb Fibre Channel z wkładkami SR oraz dwa kable światłowodowe, wielomodowe (LC/LC) o długości min. 2m.
Karta graficzna	Zintegrowana karta graficzna
Porty	5 x USB, z czego min 4szt w wersji USB 3.2 oraz jednej port USB 2.0 1x VGA Możliwość rozbudowy/rekonfiguracji o: - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express - cyfrowy port video (Display Port lub HDMI), bez użycia przejściówek z portu VGA lub USB 8
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1000W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Diagnostyka	Możliwość zainstalowania elektronicznego panelu diagnostycznego dostępnego z przodu serwera pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, zasilaczy, temperaturze.
Bezpieczeństwo	Serwer wyposażony w moduł TPM 2.0.
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub

	- przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • uwierzytelnianie oprogramowania sprzętowego PCIe z protokołem bezpieczeństwa i modelem danych (SPDM) zapewnia integralność komponentu • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power capping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory

	• obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2019, 2022 Ubuntu 20.04 LTS, 22.04 LTS Red Hat Enterprise Linux (RHEL) 8.6, 9.0 VMware ESXi 7.0 U3, 8.0, 8.0 U1/U2
Wsparcie techniczne	3-letnia gwarancja producenta w miejscu instalacji. Czas reakcji 2h w standardowe dni robocze w godzinach od 9:00 do 17:00. Przybycie serwisu do miejsca instalacji w ciągu następnego dnia roboczego od zgłoszenia usterki. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera.
Inne	Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.

9. Zasilacz awaryjny - 1 sztuka

PARAMETR	WYMAGANIA MINIMALNE
Wymagania techniczne	• Moc znamionowa jednostki nie mniej niż 1.0kW / 1.5kVA • Montaż w szafie rack • Technologia Line - interactive • Temperatura eksploatacji 0 - 40 °C • Wilgotność względna podczas pracy 0 - 95 % • Hałas słyszalny w odległości 1 m od powierzchni urządzenia 46.0dBA • Rozpraszanie ciepła w trybie online 90.0BTU/godz • Klasa ochrony IP 20
Parametry wejściowe	• Nominalne napięcie wejściowe 230V • Częstotliwość wejściowa 50/60 Hz • Zakres napięcia wejściowego w trybie podstawowym 151-302V • Inne napięcia wejściowe 220, 240
Parametry wyjściowe	• Napięcie wyjściowe 230V • Zniekształcenia napięcia wyjściowego ≤5% • Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz ±3 Hz • Inne napięcia wyjściowe 220, 240 • Typ przebiegu sinusoida • Złącza/gniazda wyjściowe: 4 x IEC 320 C13
Akumulatory i czas podtrzymania	• Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny • Czas autonomii: - powyżej 7 minut dla pełnego obciążenia - powyżej 25 minuty dla połowy obciążenia • Typowy czas ładowania 3 godziny • Oczekiwana żywotność akumulatora (lata) 3 – 5 • Baterie wymieniane na gorąco
Komunikacja i zarządzanie	• Gniazdo do montażu karty WEB/SNMP- Smart Slot x1 • Wstępnie zainstalowana karta zarządzania sieciowego do monitorowania i zarządzania UPS wraz z czujnikiem temperatury • Moduł WEB/SNMP obsługiwane protokoły komunikacyjne: IP v.6 SNMP v.3 Modbus TCP • Porty komunikacyjne: RJ45, Smart-Slot, USB • Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD • Alarm dźwiękowy Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia • Darmowe oprogramowanie do zamykania systemów operacyjnych
Certyfikaty, zgodności oraz gwarancja	• CE, EAC, RoHS • 3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulatory
Oprogramowanie	• Dostępne oprogramowanie do zarządzania/monitorigu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®

10. Oprogramowanie bazodanowe - 1 sztuka

Z uwagi na wymagania posiadanego i użytkowanego przez Zamawiającego oprogramowania dziedzinowego wymaga się zaoferowania i dostarczenia oprogramowania Microsoft SQL Server 2022 Standard Edition w postaci 1 (jednej) licencji na serwer oraz 50 (pięćdziesięciu) licencji dostępowych User CAL.

11. Oprogramowanie do backupu danych - 1 sztuka

Z uwagi na posiadane i użytkowane przez Zamawiającego oprogramowanie Acronis Cyber Protect Standard zaleca się zaoferowanie i dostarczenie oprogramowania Acronis Cyber Protect Standard w formie subskrypcji na 12 miesięcy (subskrypcja ma pozwalać na backup wszystkich uruchomionych na serwerze maszyn wirtualnych). Zamawiający dopuszcza zaoferowanie innego oprogramowania do zabezpieczania danych pod warunkiem dostarczenia licencji lub subskrypcji na wszystkie użytkowane przez Zamawiającego serwery pracujące w klastrze wirtualizacyjnym oraz spełniające poniższe wymagania:

1. Oprogramowanie musi wspierać co najmniej systemy operacyjne:
    a. dla hosta:
        i. VMware ESX/ESX(i) 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0;
        ii. Hyper-V;
        iii. Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6;
        iv. Red Hat Virtualization 4.0, 4.1;
        v. Linux KVM;
        vi. Oracle VM Server 3.0, 3.3, 3.4;
        vii. Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3.
    b. Dla maszyn wirtualnych:
        i. Windows XP (SP3) i nowsze;
        ii. Windows Server 2003 i nowsze;
        iii. Windows SBS 2011/2008, 2003/2003R2;
        iv. Windows Storage Server 2012/2012R2, 2008R2/2008/2003;
        v. Windows MultiPoint Server 2012/2011/2010;
        vi. Linux OS;
        vii. macOS.
2. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:
    a. Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www;
    b. interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego);
    c. zarządzanie procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT;
    d. definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem);
    e. możliwość zdalnej instalacji agentów kopi zapasowych z poziomu konsoli cyberochrony na maszynach z systemem operacyjnym Windows;
    f. zdalne uaktualniania agentów kopi zapasowych;
    g. zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych.
3. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:
    a. kopie zapasowe całych dysków i partycji;
    b. kopie zapasowe wybranych plików i folderów;
    c. kopia zapasowa udziałów sieciowych;

d. technologia bezagentowego wykonywania kopii zapasowej dla maszyn wirtualnych (dotyczy Hyper-V i VMWare ESXi);
e. kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory);
f. kopie zapasowe hostów Hyper-V i VMWare ESXi;
g. zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych;
h. zapis kopi zapasowych na udziały sieciowe;
i. zapis kopi zapasowych na serwer SFTP;
j. zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana;
k. wyszukiwanie plików w kopiach zapasowych;
l. szyfrowanie plików kopi zapasowych;
m. wsparcie dla technologii VSS;
n. kompresja plików kopi zapasowych;
o. replikacja kopi zapasowych na kolejny nośnik (dysk, magazyn chmurowy).

4. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:
a. odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore;
b. odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie;
c. odtworzenie całej maszyny wirtualnej;
d. odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej platformie sprzętowej;
e. odtworzenie poszczególnych plików i folderów;
f. granularne odtwarzanie baz danych Microsoft Exchange;
g. granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange;
h. wyszukiwanie i podgląd odtwarzanych wiadomości email;
i. granularne odtwarzanie baz danych Microsoft SQL;
j. granularne odtwarzanie witryn i plików Microsoft SharePoint;
k. odtwarzanie kontrolerów domeny Microsoft Active Directory;
l. przywracanie przyrostu względem danych, które już się znajdują na dysku na który przywracana jest kopia zapasowa;
m. dla hostów VMware ESXi i Hyper-V – uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej bez konieczności odtwarzania całej maszyny na hoście. Możliwość docelowego odtworzenia uruchomionej maszyny z pliku kopii zapasowej na wybranym hoście bez przerywania jej pracy.

5. Dodatkowe (obowiązkowe) wymagania związane ochroną danych:
a. ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń;
b. wbudowana ochrona antywirusowa i antymalware;
c. mechanizm ochrony przed exploitami;
d. filtrowanie adresów URL;
e. Zarządzanie produktem antywirusowym Windows Defender i Microsoft Security Essentials;
f. funkcja otrzymywania informacji o nowych zagrożeniach wraz ze wskazaniem zadań do wykonania dla konkretnego zagrożenia (m.in instalacja poprawki, wykonanie skanowania stacji);
g. mechanizm badania zdrowia dysku;
h. mechanizm ciągłej ochrony (backupu) plików zapisywanych w wybranych aplikacji lub lokalizacji. Funkcja ta musi co najmniej wspierać aplikacje z kategorii dokumentów (m.in Office, LibreOffice), inżynierii (Autocad) oraz z możliwością wskazania niestandardowej aplikacji;

i. skanowanie oprogramowania celem poszukiwania podatności. Podatności wypisane muszą być z minimum informacjami takimi jak nazwa produktu który zawiera podatność, maszyny na których znaleziono takie oprogramowanie, stopień ważności w skali CVSS;
j. filtrowanie stron na podstawie kategorii stron.

6. Przestrzeń chmurowa dostarczana wraz z oprogramowaniem musi spełniać poniższe wymagania:
   a. w przypadku uzyskania uzasadnionej pewności, że doszło do naruszenia bezpieczeństwa, producent oprogramowania bez zbędnej zwłoki dostarczy informacje o takowym naruszeniu na adres e-mail podany podczas rejestracji konta;
   b. w przypadku wyżej wymienionego naruszenia, producent podejmie kroki, aby udokumentować, naprawić i zminimalizować skutki naruszenia bezpieczeństwa w odniesieniu do danych osobowych oraz aby zapobiec jego powtórzeniu;
   c. kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich repliki muszą być przechowywane na terenie Polski;
   d. producent przechowuje dane osobowe klienta (dane osobowe oraz kopie zapasowe) przy użyciu technik szyfrowania, minimum AES-256;
   e. producent nie wykorzystuje danych osobowych klienta bez anonimizacji w środowiskach programistycznych lub testowych;
   f. producent oprogramowania przeprowadza okresowe oceny ryzyka i przeglądy co najmniej raz w roku;
   g. infrastruktura (chmurowy magazyn kopii zapasowych) jest zaprojektowana zgodnie z podejściem N+1 (to, co niezbędne +1).
   h. Producent oprogramowania jest zgodny z standardem bezpieczeństwa ISO 27001 lub SOC 2, a magazyn kopii zapasowych musi być zgodny z certyfikatami ISO 9001, ISO 27001 oraz certyfikację DCOS na minimum 4 poziomie;
   i. przestrzeń chmurowa dostarczana wraz z oprogramowaniem to minimum 250GB w ramach jednej licencji, na cały okres jej trwania.
7. Wymagania co do modelu licencjonowania rozwiązania:
   a. możliwość zakupu licencji subskrypcyjnych w okresie 1/3/5 lat;
   b. model licencjonowania oparty na maszynach fizycznych i hostach – brak limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji)

12. Przedłużenie wsparcia na oprogramowanie antywirusowe - 1 sztuka

Przedłużenie wsparcia dla posiadanej i użytkowanej przez zamawiającego licencji na oprogramowanie antywirusowe ESET PROTECT Essential ON-PREM na 2 lata. (koniec obecnej licencji to 16.03.2025; liczba chronionych stanowisk: 100) oraz zwiększenie liczby chronionych stanowisk do 120.

13. Oprogramowanie do ochrony danych (wraz z wdrożeniem i opracowaniem dokumentacji powdrożeniowej) - 1 sztuka

Zaoferowane oprogramowanie powinno spełniać poniższe wymagania:

1. Wspierany system operacyjny:
   a) Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi;
   b) Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi;
   c) MacOS 12 lub nowszy.
2. Serwer administracyjny musi obsługiwać instalację na systemie Windows Server 2016 (64-bit) i nowszym.
3. Serwer administracyjny musi obsługiwać bazy danych:
   a) MS SQL Server 2016 lub nowsze;
   b) MS SQL Express;

c) AzureSQL S3 lub nowsze.

4. Pomoc i dokumentacja programu dostępne w języku angielskim.
5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.
8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
11. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.
12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
13. Administrator musi mieć możliwość, aby tworzyć, usuwać i konta administratorów w konsoli programu.
14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.
19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
23. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.
24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
26. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
27. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.
28. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
29. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.

30. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
31. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
32. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.
33. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
34. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach.
35. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.)
36. System musi zapewniać możliwość zarządzanie szyfrowaniem dysków twardych oraz urządzeń wymiennych.
37. Licencja bezterminowa wraz z rocznym wsparciem musi umożliwiać instalację oprogramowania na 100 stanowiskach. Dodatkowo należy przeprowadzić wdrożenie oprogramowania na wskazanych przez Zamawiającego stanowiskach i opracować dokumentację powdrożeniową.

14. Dostęp przez 12 miesięcy do Platformy szkoleniowej dla 100 użytkowników - 1 sztuka

Dostęp do Platformy szkoleniowej musi zapewnić użytkownikom dostęp do wartościowej wiedzy w zakresie ochrony przed cyberzagrożeniami.

Platforma musi zawierać co najmniej:

1. dwa dedykowane bloki kursów:
    a. dotyczących bezpiecznej pracy w Internecie, w ramach których musi być dostępnych co najmniej – 12 modułów, 65 lekcji, 17 testów wiedzy
    b. dotyczących RODO, w ramach, których musi być dostępnych co najmniej 4 moduły, 30 lekcji, 5 testów wiedzy
2. statystyki i raporty dla użytkowników, grup i menadżerów;
3. możliwość dodawania własnych materiałów.

Platforma systemem chmurowym osadzonym np. w środowisku Microsoft Azure, który nie wymaga konserwacji przez Zamawiającego.

Platforma szkoleniowa musi umożliwiać zdefiniowanie konta Administratora Głównego, który musi mieć możliwość dodawania lub zaimportowania do platformy konta/kont użytkowników.

Zakres tematyczny bloku dotyczącego bezpiecznej pracy w internecie:

- Socjotechniki;
- bezpieczeństwo haseł;
- Bezpieczeństwo poczty e-mail i ochrona przed SCAM-em;
- Obrona przed phishingiem;
- Bezpieczeństwo stron WWW i przeglądarek;
- Ataki socjotechniczne z wykorzystaniem urządzeń;
- Ataki za pośrednictwem telefonu;
- Zagrożenia związane w urządzeniami mobilnymi;
- Zagrożenia związane z sieciami Wi-Fi;
- Zagrożenia w mediach społecznościowych;
- Dobre praktyki bezpieczeństwa;
- Prywatność, poufność i anonimowość w Internecie.

Zakres tematyczny bloku dotyczącego RODO:

- Incydenty i naruszenia ochrony danych
- RODO – w przykładach i praktyce stosowania

- Powierzenie przetwarzania danych i wybór dostawcy

Cechy i funkcjonalności platformy:

- możliwość szczegółowego monitorowania postępu użytkownika;
- statusy szkolenia: nierozpoczęte, w toku, ukończone;
- statusy modułu: nierozpoczęty, w toku, ukończony;
- statusy testu: nierozpoczęty, rozpoczęty, niezaliczony, zaliczony;
- brak ustalonej kolejności szkolenia, użytkownik może od razu przejść do zaliczenia testu lub zapoznawać się ze szkoleniami video według uznania lub według narzuconego w organizacji harmonogramu;
- każdy moduł zawiera krótkie streszczenie zawartości;
- każde szkolenie zawiera notatki w formie tekstowej;
- po ukończeniu materiału użytkownik wciąż ma do niego nieograniczony dostęp w ramach trwającej subskrypcji, przypisanej do organizacji;
- postęp w szkoleniu jest zapisywany, użytkownik po powrocie do danej lekcji zaczyna od momentu, w którym zakończył oglądanie materiału video;
- kurs umożliwia filtrowanie dostępnych modułów kursu (wszystkie moduły, nowe, rozpoczęte, ukończone);
- kurs pozwala użytkownikowi na ukrywanie ukończonych szkoleń;
- po ukończeniu każdego modułu szkolenia użytkownik otrzymuje certyfikat (do wydruku);
- po ukończeniu kursu użytkownik otrzymuje certyfikat (do wydruku);
- administrator platformy ma możliwość konfigurowania minimalnego postępu w kursie (tempa postępów) osiąganego przez użytkowników;
- szkolenie dostępne również w wersji mobilnej z poziomu przeglądarki, bez konieczności instalacji dodatkowego oprogramowania.

Funkcjonalności platformy związane z zarządzaniem użytkownikami:

- podział na 3 role: właściciel konta - Administrator Główny - z uprawnieniami administratora, administrator, użytkownik;
- administrator Główny jest kontem zarządzającym platformą, zintegrowanym z zewnętrznym serwisem do zarządzania subskrypcją, który jest właścicielem subskrypcji;
- konto Administratora Głównego nie wlicza się do limitu użytkowników subskrypcji, ma dostęp do wszystkich funkcji platformy. Konta Administratora Głównego nie można usunąć, dezaktywować lub obniżyć uprawnień. Edycja danych Administratora Głównego wymaga zalogowania się do zewnętrznego serwisu do zarządzania subskrypcją;
- administrator jest rolą nadawaną przez Administratora Głównego lub innego Administratora, ma dostęp do wszystkich funkcji platformy, można go usunąć, dezaktywować lub obniżyć uprawnienia;
- użytkownik - ma dostęp do swojego pulpitu oraz szkolenia w platformie, nie może zarządzać platformą. Konto użytkownika może zostać utworzone ręcznie przez dowolnego administratora lub zaimportowanie z pliku .CSV;
- możliwość nadania funkcji menedżera grupy - wiąże się z rozszerzeniem widoczności użytkownika o członków grupy, którymi zarządza (wglądu do ich danych, postępów w nauce itd.);
- platforma powinna pozwalać na śledzenie postępów użytkowników w kursie (tylko dla Administratorów oraz Menedżerów);
- platforma powinna wyświetlać listę aktywności każdego użytkownika w organizacji wraz z informacją o dacie i rodzaju aktywności;
- administrator powinien mieć możliwość podglądu postępu nauki w danym materiale szkoleniowym (lekcja lub test) użytkowników w organizacji;
- administrator oraz Menedżer mogą pobierać uzyskane przez użytkowników w organizacji certyfikaty.