

Numer sprawy: OR.272.4.2025

## Opis przedmiotu zamówienia

### Spis treści

1. UTM TYP I .....	2
2. NAS TYP I – 1 SZT .....	8
3. NAS TYP II – 1 SZT .....	10
4. OPROGRAMOWANIE DO KONTROLI POŁĄCZEŃ VPN.....	11
5. OPROGRAMOWANIE DO ARCHIWIZACJI LOGÓW .....	13
6. SERWER DO URUCHOMIENIA OPROGRAMOWANIA PODNOSZĄCEGO CYBERBEZPIECZEŃSTWO – 1 szt. ....	14
7. BIBLIOTEKA TAŚMOWA – 1 SZT.....	35
8. PRZEŁĄCZNIKI ZARZĄDZALNE - 2 SZT.....	39
9. NAS TYP III – 1 SZT .....	42
10. UPS DO KOMPUTERÓW -15 SZT .....	43
11. UPS DO SERWERÓW -1 KPL .....	45
12. SYSTEM NETWORK ACCESS CONTROL DO IZOLACJI SIECI LAN W SIEDZIBIE ZAMAWIAJĄCEGO – 130 IP .....	47
13. NAS TYP IV – 2 kpl.....	53
14. SYSTEM DO OCHRONY PRZED WYCIEKIEM DANYCH DLP – 50 LICENCJI .....	55
15. ZAKUP NOWYCH MODUŁÓW DO SYSTEMU INWENTARYZACJI AKTYWÓW – 50 LICENCJI .....	66
16. UTM TYP II .....	71
17. MINIMALNE WYMAGANIA DOTYCZĄCE WDROŻEŃ I SZKOLEŃ.....	78
A WDROŻENIE SERWERA I BIBLIOTEKI TAŚMOWEJ .....	78
B WDROŻENIE I SZKOLENIE DOTYCZĄCE OFEROWANYCH SERWERÓW NAS .....	81
C WDROŻENIE I SZKOLENIE OFEROWANYCH PRZEŁĄCZNIKÓW .....	87
D WDROŻENIE I SZKOLENIE SYSTEMU NAC DO IZOLACJI SIECI LAN W SIEDZIBIE ZAMAWIAJĄCEGO .....	87
E WDROŻENIE I SZKOLENIE SYSTEMU ZAPOBIEGANIA WYCIEKOM DANYCH I INFORMACJI (DLP) .....	88
F WDROŻENIE I SZKOLENIE OPROGRAMOWANIA AV DEDYKOWANEGO DO OCHRONY SERWERÓW .....	89
G WDROŻENIE I SZKOLENIE OPROGRAMOWANIA XDR NA SERWERACH .....	90

## 1. UTM TYP I

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	<b>Wymagania Ogólne</b>	<p>System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> <li>• Firewall.</li> <li>• Ochrony w warstwie aplikacji.</li> <li>• Protokołów routingu dynamicznego.</li> </ul>
2.	<b>Redundancja, monitoring i wykrywanie awarii</b>	<ol style="list-style-type: none"> <li>1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.</li> <li>2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</li> <li>3. Monitoring stanu realizowanych połączeń VPN.</li> <li>4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.</li> </ol>
3.	<b>Interfejsy, Dysk, Zasilanie:</b>	<ol style="list-style-type: none"> <li>1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: <ul style="list-style-type: none"> <li>• 10 portami Gigabit Ethernet RJ-45.</li> </ul> </li> <li>2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</li> <li>3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.</li> <li>4. System realizujący funkcję Firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności minimum 128 GB.</li> </ol>
4.	<b>Parametry wydajnościowe:</b>	<ol style="list-style-type: none"> <li>1. W zakresie Firewall'a obsługa nie mniej niż 1,5 mln. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.</li> <li>2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.</li> <li>3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,8 Gbps.</li> <li>4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.</li> <li>5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1,4 Gbps.</li> </ol>

		<ol style="list-style-type: none"> <li>6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.</li> <li>7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.</li> </ol>
5.	<b>Funkcje Systemu Bezpieczeństwa:</b>	<p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none"> <li>1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.</li> <li>2. Kontrola Aplikacji.</li> <li>3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.</li> <li>4. Ochrona przed malware.</li> <li>5. Ochrona przed atakami - Intrusion Prevention System.</li> <li>6. Kontrola stron WWW.</li> <li>7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.</li> <li>8. Zarządzanie pasmem (QoS, Traffic shaping).</li> <li>9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).</li> <li>10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.</li> <li>11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.</li> <li>12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.</li> <li>13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).</li> </ol>
6.	<b>Polityki, Firewall</b>	<ol style="list-style-type: none"> <li>1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</li> <li>2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: <ul style="list-style-type: none"> <li>• Translację jeden do jeden oraz jeden do wielu.</li> <li>• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.</li> </ul> </li> <li>3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</li> <li>4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.</li> <li>5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</li> <li>6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</li> <li>7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. <ul style="list-style-type: none"> <li>• Amazon Web Services (AWS).</li> <li>• Microsoft Azure.</li> <li>• Cisco ACI.</li> <li>• Google Cloud Platform (GCP).</li> </ul> </li> </ol>

		<ul style="list-style-type: none"> <li>• OpenStack.</li> <li>• VMware NSX.</li> <li>• Kubernetes.</li> </ul>
7.	Połączenia VPN	<ol style="list-style-type: none"> <li>1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: <ul style="list-style-type: none"> <li>• Wsparcie dla IKE v1 oraz v2.</li> <li>• Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).</li> <li>• Obsługa protokołu Diffie-Hellman grup 19, 20.</li> <li>• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.</li> <li>• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.</li> <li>• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</li> <li>• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.</li> <li>• Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.</li> <li>• Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.</li> <li>• Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.</li> <li>• Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.</li> <li>• Mechanizm „Split tunneling” dla połączeń Client-to-Site.</li> </ul> </li> <li>2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: <ul style="list-style-type: none"> <li>• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.</li> <li>• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.</li> <li>• 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.</li> </ul> </li> </ol>
8.	Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <ol style="list-style-type: none"> <li>1. Routingu statycznego.</li> <li>2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).</li> <li>3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.</li> <li>4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.</li> <li>5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.</li> <li>6. BFD (Bidirectional Forwarding Detection).</li> <li>7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.</li> </ol>
9.	Funkcje SD-WAN	<ol style="list-style-type: none"> <li>1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</li> <li>2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</li> </ol>
10.	Zarządzanie pasmem	<ol style="list-style-type: none"> <li>1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</li> </ol>

		<ol style="list-style-type: none"> <li>2. System daje możliwość określania pasma dla poszczególnych aplikacji.</li> <li>3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</li> <li>4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.</li> </ol>
11.	Ochrona przed malware	<ol style="list-style-type: none"> <li>1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</li> <li>2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</li> <li>3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.</li> <li>4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</li> <li>5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</li> <li>6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</li> <li>7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.</li> <li>8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.</li> <li>9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</li> <li>10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</li> </ol>
12.	Ochrona przed atakami	<ol style="list-style-type: none"> <li>1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</li> <li>2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.</li> <li>3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</li> <li>4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.</li> <li>5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</li> <li>6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</li> <li>7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.</li> <li>8. Wykrywanie i blokowanie komunikacji C&amp;C do sieci botnet.</li> <li>9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.</li> </ol>
13.	Kontrola aplikacji	<ol style="list-style-type: none"> <li>1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</li> <li>2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</li> </ol>



		<ol style="list-style-type: none"> <li>Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</li> <li>Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</li> <li>Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</li> <li>Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).</li> <li>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).</li> </ol>
14.	Kontrola WWW	<ol style="list-style-type: none"> <li>Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</li> <li>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.</li> <li>Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.</li> <li>Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</li> <li>Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</li> <li>Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</li> <li>Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</li> <li>Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</li> <li>System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji</li> </ol>
15.	Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none"> <li>System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: <ul style="list-style-type: none"> <li>Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</li> <li>Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</li> <li>Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</li> </ul> </li> <li>System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</li> <li>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.</li> <li>Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</li> </ol>
16.	Zarządzanie	<ol style="list-style-type: none"> <li>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.</li> <li>Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</li> <li>Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.</li> </ol>

		<ol style="list-style-type: none"> <li>4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</li> <li>5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</li> <li>6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</li> <li>7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</li> <li>8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</li> <li>9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</li> </ol>
17.	Logowanie	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</li> <li>4. Możliwość włączenia logowania per reguła w polityce firewall.</li> <li>5. System zapewnia możliwość logowania do serwera SYSLOG.</li> <li>6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</li> </ol>
18.	Certyfikaty	<p>Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:</p> <ul style="list-style-type: none"> <li>• EAL4 dla funkcji Firewall.</li> </ul>
19.	Serwisy i licencje	<p>Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:</p> <p>a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.</p>
20.	Gwarancja oraz wsparcie	<p>System jest objęty serwisem gwarancyjnym producenta przez okres [12] miesięcy polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie zamawiającego, realizowana przez producenta lub autoryzowanego dystrybutora w języku polskim przez okres wymaganej gwarancji.</p> <p>Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji.</p>

		<p>Do zamawianego sprzętu Wykonawca zapewni usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:</p> <p>obsługa procesu RMA u producenta,</p> <p>zdalna pomoc w skonfigurowaniu urządzenia do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producenta,</p> <p>jednorazowa podstawowa konfiguracja platformy realizowana przez inżyniera z najwyższym dostępnym poziomem certyfikacji technicznej producenta,</p> <p>dostęp do szkolenia wideo prezentującego najlepsze praktyki współpracy z suportem producenta systemu realizującego funkcję Firewall.</p> <p>Dostęp do usługi powinien być świadczony przez dedykowaną infolinię (należy podać numer telefonu) oraz przez dedykowany moduł internetowy (należy podać adres).</p> <p>Usługa ta ma być świadczona przez podmiot posiadający certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.</p> <p>Do oferty wymagane jest załączenie dokumentu sygnowanego przez Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). Certyfikat ISO 9001 podmiotu serwisującego.</p>
--	--	--

## 2. NAS TYP I – 1 SZT

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	Charakterystyka ogólna	<p>Producent i model , oferowanego NAS .</p> <p>Bezpieczne przechowywanie danych – system NAS zapewni bezpieczne przechowywane danych, chroniąc przed utratą lub uszkodzeniem danych. Szybki dostęp do danych – zapewnia szybki odczyt i zapis danych, co jest kluczowe w przypadku systemu kopii bezpieczeństwa</p> <p>Redundancja i kopie zapasowe – dzięki systemom RAID i możliwości tworzenia kopii zapasowych, NAS zwiększa odporność na awarie.</p>
2.	Procesor	Procesor wielordzeniowy osiągający w teście PassMark minimum 3950 punktów.
3.	Obudowa	Typu RACK o wysokości maksymalnie 1U wraz z kompatybilnymi szynami przesuwными do montażu w szafie rack w zestawie.
4.	Pamięć RAM	Minimum 8 GB DDR4.
5.	Ilość obsługiwanych dysków	4 dyski 3,5-calowe SATA 6 Gb/s, 3 Gb/s o pojemności maksymalnej dysku min. 22TB
6.	Zainstalowane dyski	<p>4 dyski o pojemności 8TB każdy zgodne z listą kompatybilności oferowanego serwera oraz charakteryzujące się następującymi parametrami:</p> <ul style="list-style-type: none"> <li>- prędkość obrotowa: minimum 5600 RPM,</li> <li>- pamięć cache: minimum 128MB,</li> <li>- gwarancja: minimum 36 miesięcy,</li> <li>- MTBF: minimum 1 milion.</li> </ul>
7.	Interfejsy sieciowe	<p>Minimum 2 porty 2.5 Gigabit sieci Ethernet (2,5G/1G/100M)</p> <ul style="list-style-type: none"> <li>• Obsługa VLAN i Jumbo Frame,</li> <li>• Możliwość zamontowania dodatkowej karty z interfejsami 10Gb (SFP+).</li> </ul>



8.	Porty	Minimum 2 porty USB 2.0, 2 porty USB 3.2 Gen 2, 1 port HDMI 1.4b
9.	Wskaźniki LED	HDD 1–4, stan, LAN, rozszerzenie, zasilanie
10	Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0, 1, 5, 6, 10. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania globalnego dysku zapasowego.
11	Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
12	Szyfrowanie	Możliwość szyfrowania całych woluminów kluczem AES 256 bitów.
13	System Operacyjny	Apple Mac OS 10.10 lub nowszy. Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux. IBM AIX 7, Solaris 10 lub nowszy. Microsoft Windows 7, 8, 10, 11. Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022.
14	Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
15	Usługi	Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog, możliwość tworzenia maszyn wirtualnych bezpośrednio na serwerze NAS bez zewnętrznego wirtualizatora. Obsługa automatycznego warstwowania danych tzw. auto tiering.
16	Zarządzanie dyskami	SMART, sprawdzanie złych sektorów
17	Język GUI	Polski
18	Gwarancja	Minimum 12 miesięcy gwarancji producenta.
19	Waga urządzenia bez dysków	Maksymalnie 12 kg
20	Pobór mocy	Maksymalnie 80W w trybie pracy.
21	System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
22	Liczba kont użytkowników	Minimum 4000
23	Liczba grup	Minimum 500
24	Liczba udziałów	Minimum 500
25	Maksymalna liczba migawek	Minimum 1000
26	Zasilanie	Redundantny zasilacz o mocy minimum 250W (100-240V)
27	UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.

## 3. NAS TYP II – 1 SZT

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	Charakterystyka	Producent i model, oferowanego NAS. Bezpieczne przechowywanie danych – system NAS zapewni bezpieczne przechowywane danych, chroniąc przed utratą lub uszkodzeniem danych. Szybki dostęp do danych – zapewnia szybki odczyt i zapis danych, co jest kluczowe w przypadku systemu kopii bezpieczeństwa Redundancja i kopie zapasowe – dzięki systemom RAID i możliwości tworzenia kopii zapasowych, NAS zwiększa odporność na awarie. Urządzenie będzie dedykowane również do archiwizacji logów
2.	Procesor	Procesor wielordzeniowy osiągający w teście PassMark minimum 3750 punktów.
3.	Obudowa	Typu tower (wolnostojąca) z możliwością zamknięcia każdej zatoki na dysk wykorzystując dedykowany klucz.
4.	Pamięć RAM	Minimum 8 GB DDR4.
5.	Ilość obsługiwanych dysków	4 dyski 3,5-calowe SATA 6 Gb/s, 3 Gb/s o pojemności maksymalnej dysku min. 22TB
6.	Zainstalowane dyski	4 dyski o pojemności 8TB każdy zgodne z listą kompatybilności oferowanego serwera oraz charakteryzujące się następującymi parametrami: - prędkość obrotowa: minimum 5600 RPM, - pamięć cache: minimum 128MB, - gwarancja: minimum 36 miesięcy, - MTBF: minimum 1 milion.
7.	Interfejsy sieciowe	Minimum 2 porty 2.5 Gigabit sieci Ethernet (2,5G/1G/100M) Obsługa VLAN i Jumbo Frame,
8.	Porty	Minimum 2 porty USB 2.0, 2 porty USB 3.2 Gen 2, 1 port HDMI
9.	Wskaźniki LED	HDD 1–4, stan, LAN, rozszerzenie, zasilanie
10.	Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0, 1, 5, 6, 10. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania globalnego dysku zapasowego.
11.	Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
12.	Szyfrowanie	Możliwość szyfrowania całych woluminów kluczem AES 256 bitów.
13.	System Operacyjny	Apple Mac OS 10.10 lub nowszy. Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux. IBM AIX 7, Solaris 10 lub nowszy. Microsoft Windows 7, 8, 10, 11. Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022.
14.	Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
15.	Usługi	Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog, możliwość tworzenia maszyn wirtualnych bezpośrednio na serwerze NAS bez zewnętrznego wirtualizatora, Obsługa automatycznego warstwowania danych tzw. auto tiering.
16.	Zarządzanie dyskami	SMART, sprawdzanie złych sektorów

17.	Język GUI	Polski
18.	Gwarancja	12 miesięcy gwarancji producenta
19.	Waga urządzenia bez dysków	Maksymalnie 5 kg
20.	Pobór mocy	Maksymalnie 40W w trybie pracy.
21.	System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
22.	Liczba kont użytkowników	Minimum 4000
23.	Liczba grup	Minimum 500
24.	Liczba udziałów	Minimum 500
25.	Maksymalna liczba migawek	Minimum 1000
26.	Zasilanie	Zasilacz zewnętrzny o mocy minimum 80W
27.	UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.

#### 4. OPROGRAMOWANIE DO KONTROLI POŁĄCZEŃ VPN

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	Zaawansowana ochrona stacji roboczych – rozbudowa obecnego systemu.	<p>Przedmiotem postępowania jest rozbudowa istniejącego systemu bezpieczeństwa infrastruktury teleinformatycznej o elementy zabezpieczeń dla stacji roboczych wraz z mechanizmami centralnego zarządzania.</p> <p>Dostarczone rozwiązanie do ochrony stacji roboczych musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji.</p>
2.	System ochrony dla stacji roboczych wraz z systemem centralnego zarządzania	<p>W ramach postępowania wymagany jest dostarczenie rozwiązania do ochrony stacji roboczych wraz z mechanizmami centralnego zarządzania.</p> <p>Dostarczone rozwiązanie do ochrony stacji roboczych musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji.</p>

3.	Parametry systemu ochrony dla stacji roboczych.	<p>1. Elementy systemu ochrony dla stacji roboczych powinny zapewniać następujące funkcje i mechanizmy:</p> <ul style="list-style-type: none"> <li>• Kontrola antywirusowa.</li> <li>• Funkcja analizy plików w zewnętrznym systemie Sandbox.</li> <li>• Opcja kwarantanny lokalnej plików przesłanych do Sandbox na czas analizy.</li> <li>• URL filtering w oparciu o kategorie stron z opcją definiowania wyjątków.</li> <li>• Kontrola aplikacji - w oparciu o wbudowany Firewall aplikacyjny.</li> <li>• Mechanizmy analizy podatności na stacji roboczej - pozwalające wykryć zagrożenia w systemie operacyjnym oraz zainstalowanych aplikacjach.</li> <li>• Mechanizmy szyfrowanych połączeń typu IPSec VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.</li> <li>• Mechanizmy szyfrowanych połączeń typu SSL VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.</li> <li>• Możliwość zastosowania certyfikatów cyfrowych w procesie uwierzytelnienia przy realizacji szyfrowanych połączeń.</li> <li>• Mechanizmy uwierzytelniania dwuskładnikowego</li> <li>• AntiExploit,</li> <li>• blokowanie dysków przenośnych typu USB,</li> </ul> <p>2. Poszczególne mechanizmy muszą być dostępne dla następujących systemów operacyjnych: Microsoft Windows 11 (32-bit, 64-bit Windows Serwer 2019, Windows Server 2012, Mac OS X v10.15, OS X v10.14, OS X v10.13, Linux OS, Ubuntu 16.04 i późniejsze, Red Hat 7.4 i późniejsze, CentOS 7.4 i późniejsze.</p>
		<p>3. Wymaganiem jest aby system ochrony stacji końcowej umożliwiał wysyłanie plików do platformy typu Sandbox zlokalizowanego w chmurze producenta (co najmniej w ilości 300 plików dziennie dla każdej stacji klienckiej) lub w ramach postępowania powinna zostać dostarczona komercyjna platforma typu sandbox - zainstalowana lokalnie i współpracująca z oferowanym rozwiązaniem do ochrony stacji roboczych. W ramach postępowania muszą zostać dostarczone niezbędne licencje upoważniająca zrealizowania wymaganej powyżej funkcji.</p>
	Parametry systemu centralnego zarządzania.	<p>1. Dostarczony system centralnego zarządzania aplikacjami klienckimi musi zapewniać wszystkie wymienione poniżej funkcje. Wymaga się aby elementy wchodzące w skład systemu były zrealizowane w postaci komercyjnych platform wirtualnych lub aplikacji instalowanych na systemach operacyjnych: Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2.</p> <p>2. System powinien umożliwiać automatyczną aktualizację oprogramowania zabezpieczającego na urządzeniach końcowych oraz musi zapewniać mechanizmy integracji z sieciowymi systemami bezpieczeństwa, w tym co najmniej: Firewall, Sandbox.</p> <p>3. Ponadto wymagane jest aby system zapewniał:</p> <ul style="list-style-type: none"> <li>• integrację z systemami zarządzania tożsamością użytkowników – co najmniej AD,</li> <li>• definiowanie różnych profili (wersji konfiguracji) ochrony dla różnych grup użytkowników czerpanych z AD lub definiowanych lokalnie,</li> <li>• zautomatyzowany proces zarządzania aplikacją kliencką,</li> <li>• przygotowywanie paczek instalacyjnych przynajmniej dla systemu Windows 32/64 bit i MacOS w których administrator może określić komponenty dla ochrony stacji roboczych takich jak AV, WebFiler, Skaner Podatności.</li> <li>• możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym,</li> <li>• panel, w którym wyświetlane są wyniki analizy podatności na stacjach roboczych,</li> <li>• panel w którym wyświetlane są informacje o podłączonych i zarządzanych stacjach roboczych,</li> <li>• możliwość wymuszenia patchowania wykrytych podatności na stacjach roboczych,</li> </ul>

		<ul style="list-style-type: none"> <li>• automatyczne wykrywanie stacji klienckich w grupach roboczych,</li> <li>• logowanie zdarzeń z aplikacji klienckich, możliwość ich przeglądania z funkcją filtrów oraz możliwością pobierania logów przez administratora,</li> <li>• generowanie alarmów: związanych z zarządzaniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach oraz w sytuacji zaistnienia zdarzeń związanych z aktywnością złośliwego kodu, aktywności aplikacji botnet z wykorzystaniem komunikacji C&amp;C, nieaktualnej bazy danych dla sygnatur antywirusa.</li> <li>• definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcją przypisywania uprawnień do elementów panelu konfiguracyjnego,</li> <li>• zarządzanie certyfikatami na potrzeby połączeń IPsec VPN oraz SSL VPN,</li> <li>• automatyczne wykrywanie aplikacji zainstalowanych na stacjach klienckich z możliwością filtrowania przynajmniej po producencie i nazwie aplikacji,</li> <li>• możliwość przeniesienia użytkownika przez administratora do kwarantanny i personalizację komunikatu, który wyświetli się użytkownikowi,</li> <li>• możliwość wymuszenia przeskanowania stacji klienckiej za pomocą antywirusa i skanera podatności na żądanie jak i cyklicznie, możliwość skonfigurowania weryfikacji zgodności (compliance) w celu sprawdzenia czy na stacji końcowej jest aktualna baza sygnatur dla AV, czy jest odpowiednia wersja systemu operacyjnego, czy jest uruchomiony odpowiedni proces.</li> </ul> <p>4. Administrator musi mieć możliwość wykonywania backupu i odtwarzania bazy danych, w oparciu o którą działają elementy system.</p> <p>5. Centralny system zarządzania musi zapewniać możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora lub w ramach postępowania koniecznym jest dostarczenie odpowiednio zabezpieczonego portalu, za pośrednictwem którego administrator będzie mógł dystrybuować pakiety instalacyjne.</p>
4.	Licencje oraz serwisy.	<p>W ramach postępowania wraz z konsolą centralnego zarządzania muszą zostać dostarczone niezbędne licencje upoważniające do:</p> <ol style="list-style-type: none"> <li>1. Zainstalowania i centralnego zarządzania minimum 25 licencji aplikacjami klienckimi na stacjach roboczych.</li> <li>2. Dla wskazanej powyżej ilości stacji roboczych licencje powinny obejmować: <ol style="list-style-type: none"> <li>a) Web Filtering, Skaner podatności, Remote Access, Centralne zarządzanie na okres minimum [12] miesięcy.</li> <li>b) System musi być objęty serwisem producenta przez okres minimum [12] miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.</li> </ol> </li> </ol>

## 5. OPROGRAMOWANIE DO ARCHIWIZACJI LOGÓW .

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	Dane producenta	Producent oferowanego rozwiązania
2.	Charakterystyka rozwiązania	<ol style="list-style-type: none"> <li>1. Rozwiązanie musi odbierać wiadomości Syslog</li> <li>2. Rozwiązanie musi odbierać wiadomości Trap SNMP w wersji v1, v2, v3</li> <li>3. Rozwiązanie musi nasłuchiwać Windows Event Log</li> <li>4. Rozwiązanie musi posiadać graficzny interfejs użytkownika w przeglądarce internetowej</li> <li>5. Rozwiązanie musi mieć możliwość powiadamiania użytkowników drogą emailową na bazie otrzymanych zdarzeń</li> <li>6. Rozwiązanie musi mieć możliwość uruchamiania zewnętrznych skryptów</li> <li>7. Rozwiązanie musi mieć możliwość przesyłania dalej zebranych wiadomości do innych systemów w formatach Syslog oraz Trap SNMP w wersji v1, v2, v3</li> <li>8. Rozwiązanie musi mieć możliwość eksportu zdarzeń do formatu .csv</li> <li>9. Rozwiązanie powinno umożliwiać zarządzanie politykami retencji danych zdarzeń</li> </ol>



		10. Rozwiązanie musi wspierać standard IPv4 i IPv6 11. Rozwiązanie musi wspierać przesył danych na poziomie powyżej 2 000 000 zdarzeń na godzinę 12. Rozwiązanie musi być licencjonowanie w sposób nieograniczający ilości podłączonych urządzeń przesyłających informacje 13. Rozwiązanie powinno integrować się ze Splunk 14. Rozwiązanie powinno integrować się z rozwiązaniami typu SIEM 15. Rozwiązanie musi mieć możliwość instalacji na systemach Microsoft Windows Server 2016, 2019, 2022 oraz Microsoft Windows 10, 11.
3.	Licencjonowanie	Licencja wieczysta na oprogramowanie,
4.	Usługi	Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego: - instalacja i konfiguracja rozwiązania na platformie Zamawiającego - szkolenie dla administratora rozwiązania - wsparcie w języku polskim w trybie 8x5 w dni robocze

## 6. SERWER DO URUCHOMIENIA OPROGRAMOWANIA PODNOSZĄCEGO CYBERBEZPIECZEŃSTWO – 1 szt.

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	Charakterystyka ogólna	Serwer będzie kluczowymi elementami infrastruktury IT Zamawiającego, przeznaczonym do instalacji oraz uruchomienia oprogramowania służącego podniesieniu poziomu cyberbezpieczeństwa. Serwer będzie wspierać działanie różnorodnych narzędzi dedykowanych ochronie sieci oraz zarządzaniu bezpieczeństwem, m.in. takich jak: 1. Zakup i wdrożenie rozwiązania Network Access Control (NAC) – kontrola dostępu urządzeń i użytkowników do sieci, monitorowanie i zarządzanie punktami końcowymi. 2. Zakup i wdrożenie oprogramowania do kategoryzacji i archiwizacji logów – narzędzie do gromadzenia, analizowania i przechowywania logów z infrastruktury IT. 3. Zakup i wdrożenie rozwiązania do ochrony przed wyciekiem danych (DLP) – system zapobiegający nieautoryzowanemu udostępnianiu danych wrażliwych i wyciekom informacji. 4. Zakup i wdrożenie rozwiązania do backupu i składowania danych na biblioteczce taśmowej – rozwiązanie do tworzenia kopii zapasowych i długoterminowego przechowywania danych na nośnikach taśmowych.
2.	Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji 12 dysków 3.5” Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. 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.
3.	Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 32 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Na płycie głównej powinno znajdować się 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
4.	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych

5.	<b>Procesor</b>	Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz, klasy x86, dedykowane do pracy z zaferowanym serwerem, umożliwiające osiągnięcie wyniku min. 169 w teście SPECrte2017_int_base, dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> dla konfiguracji dwuprocesorowej.
6.	<b>RAM</b>	256GB DDR5 RDIMM 5600MT/s,
7.	<b>Funkcjonalność pamięci RAM</b>	Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection (PFD)
8.	<b>Kontroler RAID</b>	Sprzętowy kontroler dyskowy, posiadający Min. 8GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących
9.	<b>Dyski twarde</b>	Zainstalowane: 2x dysk SSD SATA o pojemności min. 1.92TB, Hot-Plug 8x dysk HDD SATA o pojemności min. 8TB, Hot-Plug Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
10.	<b>Gniazda PCI</b>	Cztery sloty PCIe
11.	<b>Interfejsy sieciowe/FC/SAS</b>	Wbudowane 6 interfejsów sieciowych 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Czteroportowa karta sieciowa 1Gb Ethernet w standardzie BaseT Dwuportowa karta sieciowa 10Gb Ethernet w standardzie BaseT Czteroportowa karta 12Gb SAS HBA
12.	<b>Wbudowane porty</b>	4 porty USB w tym min: 1 port USB 3.0 z tyłu obudowy, 1 port micro USB z przodu obudowy 2 port VGA z czego jeden z przodu obudowy Możliwość rozbudowy o port RS232
13.	<b>Video</b>	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
14.	<b>Wentylatory</b>	Redundantne, Hot-Plug
15.	<b>Zasilacze</b>	Redundantne, Hot-Plug min. 1100W klasy Titanium
16.	<b>Elementy montażowe</b>	Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
17.	<b>System operacyjny/dodatkové oprogramowanie</b>	<ul style="list-style-type: none"> <li>Windows Server 2025 Standard – <b>licencja dobrana tak, aby przy oferowanych procesorach umożliwić uruchomienie 4 maszyn wirtualnych oraz 50 licencji CAL na użytkownika</b></li> <li>Microsoft Windows Server 2022 Standard lub równoważny spełniający min. poniższe wymagania:</li> <li>Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.</li> <li>Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.</li> <li>Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.</li> <li>Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.</li> <li>Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.</li> <li>Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</li> </ul>

		<ul style="list-style-type: none"> <li>• Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.</li> <li>• Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizm Hyper-Threading;</li> <li>• Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</li> <li>• Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.</li> <li>• Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.</li> <li>• Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.</li> <li>• Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</li> <li>• Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.</li> <li>• Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.</li> <li>• Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play).</li> <li>• Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</li> <li>• Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).</li> <li>• Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</li> <li>• Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</li> <li>• Możliwość migracji konfiguracji systemu Microsoft Windows Serwer 2012/2016.</li> </ul>
18.	<b>Bezpieczeństwo</b>	<p>Zatrząsek górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardej.</p> <p>Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania.</p> <p>Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</p> <p>BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła</p> <p>Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</p> <p>Moduł TPM 2.0</p> <p>Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera</p> <p>Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem</p> <p>Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).</p>
19.	<b>Karta Zarządzania</b>	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą:</p> <p>zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</p> <p>zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);</p> <p>szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;</p> <p>możliwość podmontowania zdalnych wirtualnych napędów;</p>

		<p>wirtualną konsolę z dostępem do myszy, klawiatury;</p> <p>wsparcie dla IPv6;</p> <p>wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;</p> <p>możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;</p> <p>możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;</p> <p>integracja z Active Directory;</p> <p>możliwość obsługi przez dwóch administratorów jednocześnie;</p> <p>wsparcie dla dynamic DNS;</p> <p>wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.</p> <p>możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera</p> <p>możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera</p> <p>oraz z możliwością rozszerzenia funkcjonalności o:</p> <p>Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej</p> <p>Przesyłanie danych telemetrycznych w czasie rzeczywistym</p> <p>Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze</p> <p>Automatyczna rejestracja certyfikatów (ACE)</p>
20.	<b>Oprogramowanie do zarządzania</b> – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	<p>Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</p> <p>Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych</p> <p>integracja z Active Directory</p> <p>Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta</p> <p>Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish</p> <p>Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram</p> <p>Szczegółowy opis wykrytych systemów oraz ich komponentów</p> <p>Możliwość eksportu raportu do CSV, HTML, XLS, PDF</p> <p>Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.</p> <p>Grupowanie urządzeń w oparciu o kryteria użytkownika</p> <p>Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji</p> <p>Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach</p> <p>Szybki podgląd stanu środowiska</p> <p>Podsumowanie stanu dla każdego urządzenia</p> <p>Szczegółowy status urządzenia/elementu/komponentu</p> <p>Generowanie alertów przy zmianie stanu urządzenia.</p> <p>Filtry raportów umożliwiające podgląd najważniejszych zdarzeń</p> <p>Integracja z service desk producenta dostarczonej platformy sprzętowej</p> <p>Możliwość przejęcia zdalnego pulpitu</p> <p>Możliwość podmontowania wirtualnego napędu</p> <p>Kreator umożliwiający dostosowanie akcji dla wybranych alertów</p> <p>Możliwość importu plików MIB</p> <p>Przesyłanie alertów „as-is” do innych konsol firm trzecich</p> <p>Możliwość definiowania ról administratorów</p> <p>Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów</p> <p>Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)</p>

		<p>Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta</p> <p>Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów</p> <p>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.</p> <p>Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.</p> <p>Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile</p> <p>Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.</p> <p>Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.</p> <p>Zdalne uruchamianie diagnostyki serwera.</p> <p>Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.</p> <p>Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.</p>
21.	<p><b>Oprogramowanie do monitorowania</b> – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania</p>	<p>Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <ul style="list-style-type: none"> <li>• Monitoring: <ul style="list-style-type: none"> <li>○ ilość podłączonych oraz rozłączonych systemów</li> <li>○ stan podłączonych urządzeń</li> <li>○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów</li> <li>○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia</li> <li>○ informacje o statusie gwarancji dla poszczególnych urządzeń</li> <li>○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń</li> <li>○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.</li> <li>○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych</li> <li>○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.</li> <li>○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.</li> <li>○ Zaimplementowana analityka predykcja umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.</li> <li>○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.</li> <li>○ Monitoring parametrów serwerów z informacją o minimum: <ul style="list-style-type: none"> <li>▪ Obciążeniu procesora</li> <li>▪ Zużyciu pamięci RAM</li> <li>▪ Temperaturze procesorów</li> </ul> </li> </ul> </li> </ul>



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

		<ul style="list-style-type: none"> <li>○ Generowanie raportów do plików CSV i PDF</li> <li>• Cyberbezpieczeństwo <ul style="list-style-type: none"> <li>○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.</li> <li>○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.</li> <li>○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.</li> <li>○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.</li> </ul> </li> <li>• Wspierane urządzenia <ul style="list-style-type: none"> <li>○ Urządzenie Producenta dostarczane w ramach postępowania</li> <li>○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)</li> </ul> </li> <li>• <b>Wirtualny asystent</b> <ul style="list-style-type: none"> <li>○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury;</li> </ul> </li> <li>• <b>Możliwość rozszerzenia funkcjonalności</b> <ul style="list-style-type: none"> <li>○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.</li> </ul> </li> <li>• <b>Inne</b> <ul style="list-style-type: none"> <li>○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android</li> </ul> </li> <li>• <b>Certyfikaty</b> <ul style="list-style-type: none"> <li>○ <b>Oferowana platforma musi być zaprojektowana zgodnie ze standardami:</b> <ul style="list-style-type: none"> <li>▪ ISO 27001</li> <li>▪ NIST Security and Privacy Controls for Federal Information Systems and Organization</li> <li>▪ CSA Cloud Control Matrix</li> </ul> </li> </ul> </li> </ul>
22.	<b>Certyfikaty</b>	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001. Serwer musi posiadać deklarację CE.</p> <p>Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej <a href="http://www.epeat.net">www.epeat.net</a> potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - <b>Wykonawca złoży dokument potwierdzający spełnianie wymogu.</b></p> <p>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.</p>
23.	<b>Dokumentacja użytkownika</b>	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>

24.	<p><b>Wsparcie techniczne i oprogramowanie</b> – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania</p>	<p>Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego, automatycznie tworzące zgłoszenia serwisowe w przypadku awarii.</p> <p>Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera.</p> <p>Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów.</p> <p>Konfiguracja i zaoferowany poziom wsparcia powinien po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia powinien się kontaktować z klientem w celu rozwiązania problemu.</p> <p>Oprogramowanie musi współpracować z kartą do zarządzania w urządzeniu, która będzie działać niezależnie od zainstalowanego systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit. Karta musi umożliwiać podmontowanie zdalnych wirtualnych napędów, oraz wirtualną konsolę z dostępem do myszy, klawiatury.</p> <p>Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :</p> <p>Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień.</p> <p>Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów.</p> <p>Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta.</p> <p>upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,</p> <p>możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :</p> <ul style="list-style-type: none"> <li>a. o poprawkach i usprawnieniach dotyczących aktualizacji</li> <li>b. dacie wydania ostatniej aktualizacji</li> <li>c. priorytecie aktualizacji</li> <li>d. zgodność z systemami operacyjnymi</li> <li>e. jakiego komponentu sprzętu dotyczy aktualizacja</li> <li>f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.</li> </ul> <p>wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne</p> <p>możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.</p> <p>- rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty ( dd-mm-rrrr )</p> <p>sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą ( dd-mm-rrrr ) i wersją ( rewizja wydania )</p> <p>dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml</p> <p>raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiorem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą ( dd-mm-rrrr ) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.</p>
25.	<p><b>Warunki gwarancji</b></p>	<p>Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres minimum 12 m-cy</p>

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 Producenta (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 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.

Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:

Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.

Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.

Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.

Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.

Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaze dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.

Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

26. **Ochrona serwerów** – w formularzu oferty należy podać pełną nazwę

Ochrona antywirusowa niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.

oferowanego  
oprogramowania

Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.

Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EPP i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

Rozwiązanie dla ochrony antywirusowej systemów serwerowych wspiera następujące systemy operacyjne:

- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022

Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika.

Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej

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



8. Dane zbierane przez agenta instalowanego na serwerach, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łącz sieciowych.
9. Komunikacja agentów instalowanych na stacjach roboczych, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
10. Komunikacja agentów instalowanych na stacjach roboczych, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
11. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.
12. Dane zbierane przez agentów na serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych.
14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na serwerach w środowisku informatycznym.
16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
17. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
18. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
19. Każda detekcja zawiera co najmniej następujące informacje:
  - Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
  - Data i czas wystąpienia podejrzanych zdarzeń.
  - Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.
  - Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
  - Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
  - Poziom ryzyka, określający istotność danej detekcji.
  - Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).
20. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).
21. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).
22. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
23. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
24. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.

25. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
26. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
27. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
28. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
29. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
30. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.
31. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
32. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
33. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
34. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
35. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
36. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.
37. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
38. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.
39. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransomware.
40. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
41. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
42. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
43. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
44. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
45. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
46. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
47. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.

48. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
49. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
50. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
51. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
52. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
53. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.
54. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.
55. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.
56. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
57. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
58. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
59. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
60. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
61. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
62. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego.
63. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
64. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
65. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
66. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
67. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
68. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit”.
69. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.

70. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.
71. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.
72. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
73. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.
74. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
75. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.
76. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
77. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
78. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
79. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
80. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
81. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.
82. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki.
83. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
84. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
85. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.
86. Użytkownik podczas próby przejścia na witrynę znajdującą się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
87. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
88. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.
89. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.



90. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.
91. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
92. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
93. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
94. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
95. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.
96. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
97. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
98. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
99. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
100. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
101. Moduł aktualizacji aplikacji pełni rolę mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
102. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
103. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
104. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
105. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.
106. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
107. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
108. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
109. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.



110. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
111. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
112. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.
113. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
114. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
115. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
116. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
117. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.
118. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
119. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker
120. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.
121. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.
122. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.
123. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.
124. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.
125. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)
126. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.
127. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.
128. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.
129. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.
130. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
131. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.
132. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.

133. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.
134. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
135. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
136. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.
137. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji.
138. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1, SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.
139. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.
140. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.
141. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN
142. Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD)
143. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.
144. Rozwiązanie pozwala na wygenerowanie pliku za pomocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop).
145. Wygenerowany plik może być otwarty i wykorzystany do zdalnego podłączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.
- Centralna administracja
1. Portal zarządzający jest dostępny w języku polskim.
  2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
  3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.
  4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
  5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
  6. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
  7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
  8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.

9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego połączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
10. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.
11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.
13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.
14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki.
15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach, dla których dana poprawka została wydana.
16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.
17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
21. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.
22. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
24. Profile mogą być przypisane do pojedynczych hostów lub do grup.
25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.
26. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.
27. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.
28. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.
29. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.
30. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.
31. Tworzone profile muszą dawać administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.

		<p>32. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.</p> <p>33. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego.</p> <p>34. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.</p> <p>35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.</p> <p>W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji</p>
27.	<p><b>Moduł wykrywania i reagowania na podejrzanych aktywności na urządzeniach końcowych (XDR)</b> – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania</p>	<p>System klasy EDR/XDR zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową. Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.</p> <p>Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.</p> <p>Rozwiązanie posiada możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows 10</li> <li>• Microsoft Windows 11</li> <li>• MacOS 11 "Big Sur"</li> <li>• MacOS 10.15 "Catalina"</li> <li>• MacOS 10.14 "Mojave"</li> <li>• MacOS 10.15 "Catalina"</li> </ul> <p>Rozwiązanie posiada możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:</p> <ul style="list-style-type: none"> <li>• Microsoft® Windows Server 2012</li> <li>• Microsoft® Windows Server 2016</li> <li>• Microsoft® Windows Server 2019</li> <li>• Microsoft® Windows Server 2022</li> </ul> <p>Wspierane przeglądarki internetowe:</p> <ul style="list-style-type: none"> <li>• Microsoft Edge</li> <li>• Mozilla Firefox</li> <li>• Google Chrome</li> <li>• Safari</li> </ul> <p>Rozwiązanie posiada polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze.</p> <ol style="list-style-type: none"> <li>1. Oprogramowanie instalowane na serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.</li> <li>2. Agent instalowany na serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.</li> <li>3. Agent instalowany na serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.</li> <li>4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na serwerach.</li> </ol>



5. Dane zebrane przez agenta instalowanego na serwerach są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.
6. Agent instalowany na serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:
  - dostęp do pliku;
  - tworzenie nowego procesu;
  - nawiązane połączenia sieciowe;
  - wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
  - zawartość skryptów uruchamianych na monitorowanej stacji.
7. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.
8. Dane zbierane przez agenta instalowanego na serwerach, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łącz sieciowych.
9. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
10. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
11. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.
12. Dane zbierane przez agentów na serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.
14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na serwerach w środowisku informatycznym.
16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
17. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
18. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
19. Każda detekcja zawiera co najmniej następujące informacje:
  - Listę urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
  - Data i czas wystąpienia podejrzanych zdarzeń.
  - Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.
  - Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
  - Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
  - Poziom ryzyka, określający istotność danej detekcji.
  - Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).



20. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).
21. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).
22. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
23. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
24. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
25. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
26. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrótnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
27. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
28. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
29. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
30. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.
31. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
32. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
33. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
34. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
35. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
36. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.
37. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
38. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.
39. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
40. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu antywirusowego oraz mechanizmów zarządzania podatnościami.

		41. Dodanie klucza licencyjnego skutkuje aktywowaniem dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
28.	<b>Certyfikaty i standardy</b>	<ol style="list-style-type: none"> <li>1. producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikat ISO 9001 oraz 27001 oraz usługi związane z cyberbezpieczeństwem.</li> <li>2. Producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikację ISAE 3000 assurance-based SOC 2 Type 2</li> <li>3. Producent systemu lub autoryzowany dystrybutor producenta musi być aktywnym członkiem Cloud Security Alliance</li> </ol> <p>Zespół reagowania na incydenty od producenta systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikację CREST i NCSC</p>
29.	<b>Rozszerzone wsparcie serwisowe</b>	<p>System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [12] miesięcy.</p> <p>System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:</p> <ul style="list-style-type: none"> <li>• Wsparcie telefoniczne zespołu certyfikowanych inżynierów.</li> <li>• Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.</li> <li>• Doradztwo w zakresie konfiguracji.</li> <li>• Zdalne wsparcie techniczne.</li> <li>• Pomoc w zakładaniu zgłoszeń serwisowych u producenta.</li> <li>• Przygotowanie do zdalnej konfiguracji.</li> <li>• Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.</li> <li>• Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.</li> <li>• Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.</li> <li>• Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.</li> </ul> <p><b>Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.</b></p> <p>Oferent winien przedłożyć dokumenty:</p> <ul style="list-style-type: none"> <li>• Oświadczenie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).</li> <li>• Certyfikat ISO 9001 oraz 27001 autoryzowanego podmiotu serwisującego.</li> </ul>

## 7. BIBLIOTEKA TAŚMOWA – 1 SZT.

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	<b>Ogólne</b>	Biblioteka, do sporządzania archiwum i składowania danych na taśmach, dla zwiększenia bezpieczeństwa danych,
2.	<b>Komponent</b>	Minimalne wymagania
3.	<b>Obudowa i pojemność</b>	Wysokość maksymalnie 1U do instalacji w szafie Rack. Co najmniej 9 slotów przeznaczonych na zestaw taśm.

4.	<b>Połączenie</b>	Co najmniej 1 port SAS o przepustowości co najmniej 12Gb/s w standardzie umożliwiającym podłączenie serwerów.
5.	<b>Napęd</b>	<p>Wypożyczony w co najmniej 1 sztukę napędu SAS LTO9.</p> <p>W komplecie:</p> <ul style="list-style-type: none"> <li>• 5x taśma LTO9</li> <li>• Etykiety do taśm o numerach 1-200</li> <li>• 1x taśma czyszcząca</li> </ul>
6.	<b>Wsparcie techniczne i oprogramowanie – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania</b>	<p>Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego, automatycznie tworzące zgłoszenia serwisowe w przypadku awarii.</p> <p>Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera.</p> <p>Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub Linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów.</p> <p>Konfiguracja i zaoferowany poziom wsparcia powinien po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia powinien się kontaktować z klientem w celu rozwiązania problemu.</p> <p>Oprogramowanie musi współpracować z kartą do zarządzania w urządzeniu, która będzie działać niezależnie od zainstalowanego systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit. Karta musi umożliwiać podmontowanie zdalnych wirtualnych napędów oraz wirtualną konsolę z dostępem do myszy, klawiatury.</p> <p>Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające:</p> <ul style="list-style-type: none"> <li>• Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień.</li> <li>• Predykcja analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów.</li> <li>• Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta.</li> <li>• upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,</li> <li>• możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji: <ul style="list-style-type: none"> <li>a. o poprawkach i usprawnieniach dotyczących aktualizacji</li> <li>b. dacie wydania ostatniej aktualizacji</li> <li>c. priorytecie aktualizacji</li> <li>d. zgodność z systemami operacyjnymi</li> <li>e. jakiego komponentu sprzętu dotyczy aktualizacja</li> <li>f. wszystkie poprzednie aktualizacje z informacjami jak powyżej do punktu a do punktu e.</li> </ul> </li> <li>• wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne</li> <li>• możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika aplikacji, która tego wymaga.</li> <li>• - rozpoznanie modelu oferowanego urządzenia numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr )</li> <li>• sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania)</li> </ul>

		<ul style="list-style-type: none"> <li>dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml</li> <li>raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiorem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą ( dd-mm-rrrr ) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.</li> </ul>
7.	Gwarancja	<ul style="list-style-type: none"> <li>Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres minimum 12 miesięcy</li> <li>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.</li> <li>Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych)</li> <li>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.</li> <li>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.</li> <li>Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</li> <li>Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</li> <li>Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: <ul style="list-style-type: none"> <li>Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.</li> <li>Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.</li> <li>Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.</li> <li>Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.</li> <li>Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.</li> </ul> </li> <li>Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.</li> </ul>

		<ul style="list-style-type: none"> <li>• Wymagane dołączenie do oferty dokumentu sygnowanego przez Producenta potwierdzającego, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</li> </ul>
8.	<p><b>Oprogramowanie do backupu danych na taśmach</b></p>	<ul style="list-style-type: none"> <li>• <b>Możliwość backupu licencji na 10 serwerów, 5 hostów wirtualizacji</b></li> <li>• Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich</li> <li>• Program serwerowy kompatybilny z systemami: Microsoft Windows XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology</li> <li>• Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology</li> <li>• Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików)</li> <li>• Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)</li> <li>• Automatyczny backup przy wyłączaniu komputera</li> <li>• Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i ?</li> <li>• Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows)</li> <li>• Backup baz danych i plików poczty w trybie online i offline</li> <li>• Kopie rotacyjne (wersjonowanie)</li> <li>• Zapis archiwów w otwartym formacie (ZIP 64-bit)</li> <li>• Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi</li> <li>• Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore)</li> <li>• Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej</li> <li>• Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych</li> <li>• Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO</li> <li>• Kompresja po stronie stacji roboczej</li> <li>• Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP,</li> <li>• Replikacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows)</li> <li>• Centralne sterowanie całym Systemem z jednego miejsca</li> <li>• Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników</li> <li>• Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN</li> <li>• Wysyłanie Alertów administracyjnych na e-mail</li> <li>• Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych</li> <li>• Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki</li> <li>• Automatyczna aktualizacja oprogramowania na komputerach zdalnych</li> <li>• Bezterminowa licencja - licencja nie może być ograniczona czasowo</li> <li>• Interfejs, instrukcja i pomoc techniczna w języku polskim</li> </ul>



## 8. PRZEŁĄCZNIKI ZARZĄDZALNE - 2 SZT.

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	<b>Charakterystyka Ogólna</b>	<p>Przełącznik zarządzalny do szafy rack</p> <ol style="list-style-type: none"> <li>Przełącznik musi posiadać minimum 48 portów RJ45 o minimalnej prędkości 1Gb/s.</li> <li>Dodatkowo przełącznik musi posiadać minimum 4 porty SFP+ o prędkości minimum 10Gb/s.</li> <li>Przełącznik musi posiadać port konsolowy.</li> <li>Porty Ethernet muszą oferować zasilanie urządzeń, które wymagają wartości 30W jako mocy zasilania za pomocą technologii PoE.</li> <li>Przełącznik musi oferować funkcje odłączania i przywracania zasilania do urządzenia podłączonego przez port PoE, gdy nie zostanie zauważony żaden pakiet wysłany przez to urządzenie.</li> <li>Zasilacz przełącznika musi oferować minimum 300W mocy na zasilanie portów PoE.</li> <li>Przełącznik musi być, posiadać ochronę wszystkich portów przed przepięciami do 6000V.</li> <li>Przełącznik musi posiadać ochronę przeciwzwarciową.</li> <li>Przełącznik musi posiadać ochronę przeciw przeciążeniową PoE.</li> <li>Zasilacz przełącznika musi posiadać ochronę przeciw przegrzaniem.</li> <li>Zasilacz przełącznika musi posiadać przed nadmiernym napięciem.</li> <li>Przełącznik musi umożliwiać montaż w standardowej szafie rack 19" za pomocą dostarczonych do zestawu uchwytów montażowych.</li> <li>Przepustowość przełącznika nie może być mniejsza niż 176Gb/s.</li> <li>Szybkość przełączania ramek wewnątrz przełącznika nie może być mniejsza niż 130,9Mp/s.</li> <li>Przełącznik musi posiadać wsparcie dla technologii 802.1Q.</li> <li>Przełącznik musi posiadać przynajmniej wsparcie dla takich protokołów jak: <ol style="list-style-type: none"> <li>MAC VLAN</li> <li>IP VLAN</li> <li>QinQ</li> <li>Voice VLAN</li> </ol> </li> <li>Przełącznik musi posiadać możliwość tworzenia tras statycznych dla protokołu IPv4 jak i dla IPv6.</li> <li>Przełącznik musi posiadać obsługę przynajmniej takich protokołów przesyłania grupowego takich jak: <ol style="list-style-type: none"> <li>IGMP v1</li> <li>IGMP v2</li> <li>IGMP v3</li> <li>MLD</li> <li>PIM-DM</li> <li>PIM-SSM</li> </ol> </li> <li>Przełącznik musi posiadać ochronę podszywania w grupach multimijsyjnych za pomocą przynajmniej takich protokołów jak: <ol style="list-style-type: none"> <li>IGMP v1</li> <li>IGMP v2</li> <li>IGMP v3</li> <li>MLD v1</li> <li>MLD v2</li> </ol> </li> <li>Przełącznik musi posiadać możliwość tworzenia dynamicznych tras za pomocą przynajmniej takich protokołów jak: <ol style="list-style-type: none"> <li>RIP</li> <li>RIPNG</li> <li>OSPF</li> </ol> </li> </ol>

- d. OSPF v3
- 21. Przełącznik musi przynajmniej umożliwiać agregację portów za pomocą protokołu LACP.
- 22. Przełącznik musi przynajmniej posiadać agregację portów w trybie:
  - a. Pasywnym
  - b. Aktywnym
  - c. Statycznym
- 23. Przełącznik musi obsługiwać technologię drzewa rozpinającego w przynajmniej w wersji:
  - a. STP (IEEE 802.1d)
  - b. RSTP (IEEE 802.1w)
  - c. MSTP (IEEE 802.1s)
- 24. Przełącznik musi obsługiwać technologię ERPS.
- 25. Przełącznik musi przynajmniej umożliwiać przeciwdziałanie burzom rozgłoszeniowym jak i multiemisijnym.
- 26. Przełącznik musi posiadać ochronę przed zapętleniem ruchu poprzez automatyczne zablokowanie portu.
- 27. Przełącznik musi posiadać możliwość uruchomienia serwera DHCP.
- 28. Serwer DHCP musi przynajmniej posiadać możliwość stworzenia pul adresowych jak i statycznego przypisania adresu MAC do wskazanego adresu IP.
- 29. Przełącznik musi posiadać ochronę przed podszywaniem się serwer DHCP.
- 30. Przełącznik musi posiadać możliwość uwierzytelniania przynajmniej za pomocą protokołów takich jak:
  - a. RADIUS
  - b. TACACS+
  - c. 802.1X
- 31. Przełącznik musi posiadać ochronę przed odmową usługi.
- 32. Przełącznik musi posiadać ochronę ARP.
- 33. Przełącznik musi posiadać ochronę źródłowych adresów IP.
- 34. Przełącznik musi posiadać obsługę przynajmniej protokołów zarządzających takich jak:
  - a. IEEE 802.1ag CFM
  - b. IEEE 802.3ah EFM OAM
- 35. Przełącznik musi przynajmniej posiadać możliwość zarządzania za pomocą protokołów takich jak:
  - a. Telnet
  - b. SSH
  - c. Port konsolowy
- 36. Przełącznik musi posiadać możliwość badania stanu urządzenia za pomocą przynajmniej takich protokołów jak:
  - a. SNMP v1
  - b. SNMP v2
  - c. SNMP v3
  - d. RMON
- 37. Przełącznik musi posiadać możliwość pozyskiwania zdarzeń z urządzenia przynajmniej za pomocą protokołu syslog.
- 38. Przełącznik musi posiadać wsparcie dla protokołu LLDP.
- 39. Przełącznik musi przynajmniej posiadać możliwość wybrania portu, na którym będzie działać protokołu LLDP.
- 40. Przełącznik musi umożliwiać konfigurację protokołu QoS.
- 41. Przełącznik musi umożliwiać ustawienie polityk QoS w przynajmniej takich trybach jak:
  - a. SP
  - b. WRR
  - c. WFQ

		<p>42. Przełącznik musi przynajmniej posiadać możliwość wskazania czy dany port będzie wykorzystywany do wysyłania, odbierania lub do obustronnej transmisji pakietów LLDP na wskazanym porcie.</p> <p>43. Przełącznik musi przynajmniej posiadać możliwość pobierania i wysyłania konfiguracji za protokołu TFTP.</p> <p>44. Przełącznik musi przynajmniej posiadać możliwość konfiguracji listy dostępowej, która umożliwiałaby blokowanie lub zezwalanie dostępu do urządzenia za pomocą takich parametrów jak:</p> <ol style="list-style-type: none"> <li>Adres MAC źródłowy</li> <li>Adres MAC docelowy</li> <li>Adres IP źródłowy</li> <li>Adres IP Docelowy</li> </ol> <p>45. Przełącznik musi przynajmniej posiadać możliwość zarządzania urządzeniem za pomocą protokołu TR-069.</p> <p>46. Przełącznik musi posiadać dostarczony przez producenta na urządzeniu panel administracyjny.</p> <p>47. Panel administracyjny musi być dostępny z poziomu przeglądarki.</p> <p>48. Panel administracyjny musi posiadać możliwość łączności za pomocą przynajmniej protokołów takich jak:</p> <ol style="list-style-type: none"> <li>HTTP</li> <li>HTTPS</li> </ol> <p>49. Panel administracyjny musi posiadać polską wersję językową.</p> <p>50. Panel administracyjny musi umożliwiać zmianę priorytetu portów PoE.</p> <p>51. Panel administracyjny musi umożliwiać regulowanie maksymalnej ilości Watów jaka może użyć urządzenie zasilane za pomocą portu PoE.</p> <p>52. Panel administracyjny musi umożliwiać wyłączenie zasilania dla wybranego portu Ethernet.</p> <p>53. Panel administracyjny musi umożliwiać monitorowanie wartości takich jak napięcie i moc aktualnie podłączonego urządzenia za pomocą zasilania PoE.</p> <p>54. Panel administracyjny musi umożliwiać monitorowanie aktualnej temperatury modułów zasilających porty PoE.</p> <p>55. Panel administracyjny musi umożliwiać monitorowanie aktualnego obciążenia modułów zasilających porty PoE.</p> <p>56. Panel administracyjny musi umożliwiać wyznaczanie harmonogramu czasowe, w którego ramach można określić, w jakich godzinach i dniach przełącznik nie będzie dostarczał zasilania do urządzenia podłączone po porcie PoE.</p> <p>57. Panel administracyjny musi umożliwiać diagnozowanie łączności przynajmniej za pomocą takich technologii jak:</p> <ol style="list-style-type: none"> <li>Ping</li> <li>Tracert</li> </ol> <p>58. Panel administracyjny musi umożliwiać eksportowanie i importowanie pliku konfiguracyjnego urządzenia.</p> <p>59. Przełącznik musi posiadać możliwość podłączenia urządzenia do chmury producenta.</p>
2.	Certyfikaty i standardy	<ul style="list-style-type: none"> <li>ISO 9001</li> <li>ISO 50001</li> <li>CE</li> <li>ROHS</li> </ul>
3.	Rozszerzone wsparcie serwisowe	<p>System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [36] miesięcy.</p> <p>System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:</p> <ul style="list-style-type: none"> <li>Wsparcie telefoniczne zespołu certyfikowanych inżynierów.</li> <li>Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.</li> </ul>

		<ul style="list-style-type: none"> <li>Doradztwo w zakresie konfiguracji.</li> <li>Zdalne wsparcie techniczne.</li> <li>Pomoc w zakładaniu zgłoszeń serwisowych u producenta.</li> <li>Przygotowanie do zdalnej konfiguracji.</li> <li>Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.</li> <li>Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.</li> <li>Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.</li> <li>Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.</li> </ul> <p><b>Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.</b></p> <p>Oferent winien przedłożyć dokumenty:</p> <ul style="list-style-type: none"> <li>Oświadczenie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).</li> <li>Certyfikat ISO 9001 oraz 27001 autoryzowanego podmiotu serwisującego.</li> </ul>
--	--	--

## 9. NAS TYP III – 1 SZT

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	Charakterystyka	Bezpieczne przechowywanie danych – system NAS zapewni bezpieczne przechowywane danych, w postaci kopii wyniesionej, w lokalizacji poza główną serwerownią, chroniąc przed utratą lub uszkodzeniem danych. Szybki dostęp do danych – zapewnia szybki odczyt i zapis danych, co jest kluczowe w przypadku systemu kopii bezpieczeństwa Redundancja i kopie zapasowe – dzięki systemom RAID i możliwości tworzenia kopii zapasowych, NAS zwiększa odporność na awarie. Urządzenie będzie dedykowane również do archiwizacji logów
2.	Procesor	Wielordzeniowy procesor o architekturze 64-bitowej.
3.	Obudowa	Typu desktop (wolnostojąca).
4.	Pamięć RAM	Minimum 16GB DDR4 ECC (1 x 16GB lub 2 x 8GB). Model pamięci musi znajdować się na oficjalnej liście zgodności producenta – nie zezwala się na stosowanie zamienników.
5.	Ilość obsługiwanych dysków	Minimum 8 dysków o maksymalnej pojemności nie mniejszej niż 18TB każdy, po podłączeniu modułów rozszerzających minimum 18 dysków.
6.	Zainstalowane dyski	8 dysków o pojemności 8TB każdy zgodnych z listą kompatybilności oferowanego serwera oraz charakteryzujących się następującymi parametrami: <ul style="list-style-type: none"> <li>- prędkość obrotowa: minimum 7200 RPM,</li> <li>- gwarancja: minimum 36 miesięcy,</li> <li>- MTBF: minimum 1 milion,</li> <li>- możliwość aktualizacji oprogramowania dysku bezpośrednio z poziomu systemu operacyjnego serwera NAS.</li> </ul>
7.	Interfejsy sieciowe	Minimum 4 porty 1GbE RJ-45. Obsługa agregacji łączy.
8.	Porty	Minimum 2 porty USB 3.2. Minimum 1 gniazdo rozszerzenia służące do podłączania jednostek rozszerzających.

9.	Wskaźniki LED	Status, HDD, zasilanie, LAN
10.	Obsługa RAID	Podstawowy, RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare.
11.	Funkcje RAID	Możliwość zwiększania pojemności poprzez wymianę dysków na większe. Migracja poziomu RAID w trybie online dla minimum RAID 1 i RAID 5.
12.	Szyfrowanie	Możliwość szyfrowania wybranych udziałów sieciowych.
13.	Protokoły	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP
14.	Usługi	<p>1. Serwer VPN, Stacja monitoringu, Windows ACL, Integracja z Windows Active Directory, Firewall, Serwer plików, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Usługa DDNS, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki (min. 65 tys. w cały systemie), możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów.</p> <p>2. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 7 lub nowszym według harmonogramu z możliwością zarządzania z poziomu centralnej konsoli dostępnej lokalnie oraz zdalnie, przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Dane z kopii zapasowych muszą być redukowane poprzez globalną deduplikację po stronie miejsca przechowywania. Licencja musi umożliwiać podłączanie kolejnych komputerów do systemu kopii zapasowej bez limitu.</p> <p>3. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klastr obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora.</p>
15.	Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
16.	Język GUI	Polski
17.	Gwarancja i serwis	Minimum 12 miesięcy gwarancji Next Business Day On-site producenta na cały zestaw złożony z serwera, dysków i akcesoriów z gwarantowanym terminem naprawy sprzętu przez dedykowanego inżyniera w przypadku awarii sprzętowej na następny dzień roboczy z opcją pozostawienia uszkodzonego nośnika.
18.	Waga bez dysków	Maksymalnie 10 kg
19.	Typowy pobór mocy podczas pracy	Maksymalnie 130W
20.	Certyfikaty	CE, FCC
21.	System plików	Dyski wewnętrzne: BTRFS
22.	Szyfrowanie	Mechanizm szyfrowania sprzętowego
23.	Zasilacz	Pojedynczy zasilacz wewnętrzny o mocy minimum 200W.
24.	Chłodzenie	Minimum 2 wentylatory z możliwością regulowania prędkości obrotowej oraz wymiany w urządzeniu podczas pracy.

## 10. UPS DO KOMPUTERÓW -15 SZT

L.P.	Parametr	Charakterystyka (wymagania minimalne)
1.	Moc pozorna	minimum 2000VA



2.	Moc rzeczywista	minimum 1200W
3.	Technologia	minimum line-interactive
4.	Typ obudowy	tower
<b>Wejście</b>		
5.	Napięcie wejściowe	minimum 220/230/240 VAC
6.	Zakres napięcia wejściowego	minimum 140-300 VAC
7.	Częstotliwość	minimum 50/60 Hz (auto wykrywanie)
<b>Wyjście</b>		
8.	Regulacja napięcia	minimum '+/- 10 %
9.	Kształt napięcia wyjściowego	minimum symulowana sinusoida
10.	Typowy czas przełączania	2-6 ms
<b>Baterie</b>		
11.	Baterie wewnętrzne w UPS	minimum 2x 12V 9Ah; szczelne, bezobsługowe
12.	Czas podtrzymania (dla 75% Pmax)	minimum 5 minut
<b>Pozostałe</b>		
13.	Wejście zasilania	kabel zamontowany na stałe w obudowie UPS zakończony wtykiem PL/FR
14.	Ilość i typ gniazd wyjściowych	minimum 4 gniazda Schuko (z podtrzymaniem)
15.	Stabilizacja napięcia AVR Boost & Buck	wymagana
16.	Filtr RJ45	wymagany
17.	Ładowanie w trybie wyłączenia	wymagane
18.	Funkcja autorestartu po powrocie zasilania	wymagana
19.	Funkcja zimnego startu	wymagana
20.	Sygnalizacja	Dźwiękowa, Wyświetlacz LCD
21.	Alarmy dźwiękowe	minimum Tryb bateryjny, Rozładowana bateria, Przeciążenie, Awaria
22.	Informacje wyświetlane na panelu LCD	minimum napięcie wejściowe i wyjściowe, poziom obciążenia, poziom naładowania baterii praca z sieci/baterii, przeciążenie, niski poziom baterii
23.	Alarmy dźwiękowe	minimum Tryb bateryjny, Rozładowana bateria, Przeciążenie, Awaria
24.	Interfejs komunikacyjny	USB
25.	Zabezpieczenia	Minimum ochrona przed zwarcieniem, przeciążeniem, rozładowaniem
26.	Waga UPS	do 12 kg
27.	Wymiary UPS	nie większe niż: wysokość 205 mm; szerokość 146 mm, głębokość 398 mm
28.	Gwarancja	minimum 12 miesięcy na elektronikę i 12miesięcy na akumulatory;
29.	Serwis	autoryzowany serwis producenta zlokalizowany w Polsce.
		naprawa w maksymalnie 7 dni roboczych

		serwis realizowany w systemie door to door
30.	Oprogramowanie	oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS wsparcie dla systemów: Windows, Linux wymagane wsparcie producenta w języku polskim (telefoniczne oraz mailowe)
31.	Certyfikaty producenta (załączyć do oferty)	deklaracja zgodności CE -z załączyć do oferty

## 11. UPS DO SERWERÓW -1 KPL

L.p.	Parametr	Charakterystyka (wymagania minimalne)
1.	Moc pozorna	minimum 10000VA
2.	Moc rzeczywista	minimum 10000W
3.	Technologia	on-line (VFI), podwójna konwersja
4.	Sprawność przy pracy sieciowej	> 95 %
5.	Sprawność przy pracy baterijnej	> 92 %
6.	Typ obudowy	rack/tower
<b>Wejście</b>		
7.	Napięcie wejściowe	minimum 208/220/230/240 VAC
8.	Częstotliwość napięcia wejściowego	minimum 46~54 Hz lub 56~64 Hz
9.	Zakres napięcia wejściowego	minimum 110 ÷ 300 V AC ± 3% przy 50% obciążenia oraz 176 ÷ 300VAC ± 3 % dla 100% obciążenia
10.	Kształt napięcia wyjściowego	sinusoidalny
11.	Czas przełączania sieć – bateria	0ms
12.	Współczynnik odkształceń prądu wejściowego THDi	<3% przy 100% obciążenia
<b>Wyjście</b>		
13.	Napięcie wyjściowe	minimum 208/220/230/240 VAC
14.	Częstotliwość napięcia wyjściowego	minimum 50Hz/60Hz ± 0,1Hz
15.	Kształt napięcia wyjściowego na pracy baterijnej	sinusoidalny
16.	Współczynnik odkształceń prądu wejściowego THD	≤ 2 % (obciążenie liniowe); ≤ 6 % (obciążenie nieliniowe)
17.	Baterie wewnętrzne w UPS lub w zewnętrznym module baterijnym	minimum 12V 9Ah; szczelne, bezobsługowe
18.	Czas podtrzymania dla obciążenia 100% - przy zastosowaniu wewnętrznych baterii lub w maksymalnie 1 zewnętrznym module baterijnym producenta UPS	minimum 4 minuty
<b>Pozostałe</b>		
19.	Prąd ładowania baterii	minimum od 1A do 4A (regulowane)
20.	Współpraca z 20 bateriami	wymagane
21.	Wejście zasilania	listwa zaciskowa / terminal śrubowy
22.	Ilość i typ gniazd wyjściowych	listwa zaciskowa / terminal śrubowy
23.	Obciążalność w trybie sieciowym AC	100%~110%:10min; 110%~130%:1min; >130%:1s
24.	Sygnalizacja	Wyświetlacz LCD (obracany)

25.	Informacje wyświetlane na panelu LCD	minimum poziom obciążenia (w %), poziom naładowania baterii (w %), praca z sieci/baterii/ładowanie baterii, przeciążenie, niski poziom baterii, bateria nie podłączona lub błąd baterii, tryb ECO/Bypass, napięcie wej/wyj, częstotliwość wej/wyj, błąd + numer błędu, czas podtrzymania bateryjnego, wyłączenie dźwięku,
26.	Możliwość podłączenia dodatkowych, zewnętrznych modułów bateryjnych (producenta)	wymagane
27.	Interfejs komunikacyjny	RS232, USB, SNMP
28.	Możliwość zastosowania karty SNMP w innych rozwiązaniach 1-fazowych i 3-fazowych tego samego producenta	wymagane
29.	Zabezpieczenia	minimum przeciwzwarciove, przeciwprzepięciowe, przeciążeniowe
30.	Złącze EPO	wymagane
31.	Zewnętrzny bypass serwisowy w wersji rack, tego samego producenta co oferowany UPS	wymagany
32.	Czujnik środowiskowy SNMP (temperatury i wilgotności) kompatybilny z oferowanym zasilaczem UPS	wymagany
33.	Wsporniki do montażu w szafie rack	wymagane
34.	Waga UPS	do 20 kg
35.	Wymiary UPS - wersja RACK	nie większe niż: wysokość 88 mm; głębokość 620 mm, szerokość 440 mm
36.	Waga pojedynczego Modułu Bateryjnego - jeżeli występuje	do 80 kg
37.	Wymiary pojedynczego Modułu Bateryjnego - wersja RACK - jeżeli występuje	nie większe niż: wysokość 135 mm; głębokość 720 mm, szerokość 440 mm
38.	Gwarancja	minimum 12 miesięcy na elektronikę i 12 miesięcy na akumulatory;
39.	Serwis	autoryzowany serwis producenta zlokalizowany w Polsce.
		naprawa w maksymalnie 5 dni (w dni robocze)
		serwis realizowany w systemie onsite - w miejscu instalacji urządzenia
		gwarancja realizowana wyłącznie przez Autoryzowany Serwis Producenta
40.	Oprogramowanie	oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS
		wsparcie dla systemów: Windows, Linux

		wymagane wsparcie producenta w języku polskim (telefoniczne oraz mailowe)
41.	Możliwość monitorowania i konfiguracji UPS przez przeglądarkę WWW	wymagane
<b>Usługi</b>		
42.	Usługa dostawy z wniesieniem, montaż BYPASS (w odległości nie większej niż 3m od UPS), podłączenie BYPASS (do przygotowanej instalacji elektrycznej - wyprowadzonych kabli wej/wyj zasilania), podłączenie BYPASS do UPS, podłączenie modułów bateryjnych (jeżeli występują), pierwsze uruchomienie, szkolenie z obsługi.	wymagane
<b>Dokumenty</b>		
43.	Oświadczenia / dokumenty (załączyć do oferty)	a. deklaracja zgodności CE b. dokument sygnowany przez producenta lub wyłącznego dystrybutora, poświadczający, iż usługi podłączenia i uruchomienia realizowana będą wyłącznie przez autoryzowany serwis producenta
<b>Wyposażenie dodatkowe</b>		
44.	Listwa PDU do zasilacza UPS 10kW - wymagania minimalne	minimum 2 x Gniazdo okrągłe z bolcem 16A/230V + 8 x Gniazdo komputerowe typu IEC320C13 10A/230V + 2 x Gniazdo komputerowe typu IEC320C19 16A/230V, Gniazda z bolcem obrócone o kąt 45° względem obudowy Gniazda zabezpieczone przed wetknięciem przypadkowych przedmiotów. Gniazda podzielone na dwa bloki. Każdy blok zabezpieczony wyłącznikiem nadmiarowo-prądowym MCB z charakterystyką C i ograniczeniem do 16A Listwa w kolorze czarnym (RAL9005) Obudowa aluminiowa anodyzowana w kolorze naturalnym. Wsporniki do montażu listwy w 4 płaszczyznach. Kabel zasilający długości 2m, typu H05VV-F.3G6mm <sup>2</sup> zakończony końcówkami oczkowymi M5. Maksymalne obciążenie 32A (7360 W). Stopień ochrony IP20. Deklaracja zgodności CE.
45.	Listwa PDU tego samego producenta co UPS	wymagane

## 12. SYSTEM NETWORK ACCESS CONTROL DO IZOLACJI SIECI LAN W SIEDZIBIE ZAMAWIAJĄCEGO – 130 IP

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	Dane producenta /model	Producent oferowanego rozwiązania /model i wersja modelu
2.	Opis funkcjonalności rozwiązania	<p>Wymagane jest dostarczenie rozwiązania typu NAC (Network Access Control), służącego do monitorowania sieci lokalnych w celu uwidocznienia pracujących w nich urządzeń oraz wykrywania nowych urządzeń pojawiających się w sieci, w czasie rzeczywistym. Rozwiązanie musi raportować aktualny stan każdego urządzenia, z uwzględnieniem takich atrybutów, jak adres MAC, adres IP, nazwa hosta, system operacyjny, itp., pozyskując te informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą siecią (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.).</p> <p>Rozwiązanie ma za zadanie zapewnić, aby tylko urządzenia, których aktualny stan spełnia zdefiniowaną przez administratora politykę bezpieczeństwa, mogły bez ograniczeń ze strony NAC pracować w sieci lokalnej. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenia, których aktualny stan nie spełnia danych warunków polityki bezpieczeństwa (np. nowe, po raz pierwszy pojawiające się urządzenie lub</p>

		<p>stacja robocza z wyłączonym oprogramowaniem antywirusowym). Mechanizm kwarantanny powinien umożliwiać całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym, jak również blokowanie częściowe, w zakresie definiowanym przez administratora (przez wskazanie adresów IP, z którymi urządzenie może się komunikować). Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej.</p> <p>Rozwiązanie musi posiadać funkcjonalność typu Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów.</p>
3.	Wymagania ogólne rozwiązania NAC	<ol style="list-style-type: none"> <li>1. Ma zapewnić widoczność i monitorowanie wszystkich urządzeń pracujących w sieci lokalnej oraz powiadamiać o nowych urządzeniach pojawiających się w sieci.</li> <li>2. Musi zapewniać automatyczne blokowanie komunikacji sieciowej między nowym, niezaufanym urządzeniem a zaufanymi, zarządzanymi urządzeniami pracującymi w sieci.</li> <li>3. Musi umożliwiać sprawdzanie statusu aktualizacji oprogramowania antywirusowego i poprawek systemowych na zarządzanych stacjach roboczych Windows i w przypadku niespełniania określonych wymagań, automatycznie ograniczać tym stacjom roboczym możliwość pracy w sieci.</li> <li>4. Musi umożliwiać odbieranie komunikatów bezpieczeństwa z innych systemów bezpieczeństwa (np. firewalla) i automatyczne blokowanie na tej podstawie wskazanych urządzeń w sieci.</li> <li>5. Musi mieć funkcję wykrywania faktu skanowania urządzeń i portów wykonywanego przez urządzenie w sieci lokalnej i automatycznie blokować takie urządzenie, aby zapobiegać potencjalnemu szerzeniu się malware.</li> <li>6. Stosowany mechanizm blokowania musi wykorzystywać protokół ARP i działać całkowicie niezależnie od innych elementów infrastruktury sieciowej.</li> <li>7. Rozwiązanie musi działać bezagentowo, bez konieczności instalowania jakichkolwiek agentów na urządzeniach w sieci oraz bez konieczności dokonywania zmian w infrastrukturze sieciowej.</li> <li>8. Rozwiązanie musi umożliwiać wysyłanie alertów do administratora za pomocą e-maila oraz SMS</li> <li>9. Rozwiązanie musi być zarządzane przez interfejs webowy, obsługiwany przeglądarką internetową</li> <li>10. <b>Wymaga się, aby rozwiązanie było dostarczone w postaci maszyny wirtualnej na platformę VMware o Hyper-V. System musi pozwalać na monitorowanie co najmniej 10 sieci VLAN i monitorowanie łącznie co najmniej 500 urządzeń.</b></li> <li>11. <b>Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej i dostarczone z licencją pozwalającą na monitorowanie 130 urządzeń wraz ze wsparciem technicznym na okres na minimum 12 m-cy</b></li> </ol>
4.	Wymagania szczegółowe – monitorowanie podsieci	<ol style="list-style-type: none"> <li>1. Rozwiązanie musi w czasie rzeczywistym raportować widoczność wszystkich urządzeń pracujących w monitorowanych podsieciach.</li> <li>2. Rozwiązanie musi wykrywać nowe nieznane urządzenie, dołączające się do sieci LAN lub WLAN, w czasie nie dłuższym, niż 5 sekund oraz wysłać powiadomienie mailowe do administratora</li> <li>3. Rozwiązanie musi wykrywać przypadki skanowania urządzeń i portów w monitorowanych podsieciach i blokować urządzenie inicjujące takie skanowanie</li> <li>4. Rozwiązanie musi posiadać funkcję pułapki sieciowej (honeypot), symulującą w każdej monitorowanej podsieci standardowe usługi sieciowe, co najmniej: ssh, telnet, ftp i smb. Rozwiązanie musi rejestrować każdą próbę zalogowania się do takiej symulowanej usługi, zapisując użytą nazwę użytkownika, hasło użytkownika i źródłowy MAC/IP.</li> <li>5. Rozwiązanie musi określać aktualny stan każdego urządzenia, pozyskując informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.) oraz odświeżać te informacje cyklicznie. Musi być możliwość wykorzystania pozyskanych informacji do definiowania polityk bezpieczeństwa.</li> <li>6. Rozwiązanie musi chronić przed podszywaniem się pod adres MAC (MAC spoofing), umożliwiając zdefiniowanie „odcisku palca” (fingerprint) dla każdego zaufanego urządzenia. Odcisk palca musi</li> </ol>



		<p>być kombinacją co najmniej: adresu MAC, adresu IP, nazwy hosta, nazwy systemu operacyjnego, otwartych portów TCP. Jeśli przeprowadzana cyklicznie weryfikacja odcisku palca wykaże jego zmianę, urządzenie powinno zostać zablokowane.</p> <p>7. Rozwiązanie musi obsługiwać VLANy, tj. umożliwiać monitorowanie przez jeden fizyczny interfejs sieciowy wielu podsieci, zdefiniowanych jako VLANy</p>
5.	Wymagania szczegółowe – polityka bezpieczeństwa	<p>1. Rozwiązanie musi umożliwiać definiowanie polityki bezpieczeństwa, czyli określenie przez administratora, jakie warunki musi spełniać aktualny stan urządzenia, aby uzyskało ono określony dostęp do sieci.</p> <p>2. W definiowaniu polityki bezpieczeństwa musi być możliwość wykorzystania informacji o aktualnym stanie urządzenia, pozyskanych bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.), poprzez integrację z tymi systemami.</p> <p>3. Polityka bezpieczeństwa musi umożliwiać przypisanie do urządzenia jednego z trzech trybów dostępu do sieci:</p> <ol style="list-style-type: none"> <li>pełny dostęp</li> <li>blokowanie (całkowity brak dostępu)</li> <li>ograniczony dostęp</li> </ol> <p>4. Zakres ograniczonego dostępu powinien być definiowany przez administratora, np. w postaci list ACL, określających, do których adresów IP i portów urządzenie ma dostęp. Musi być możliwość zdefiniowania wielu różnych zakresów ograniczonego dostępu.</p> <p>5. Rozwiązanie powinno automatycznie sprawdzać, które warunki polityki bezpieczeństwa spełnia urządzenie i na tej podstawie przypisywać do urządzenia właściwy zakres dostępu.</p> <p>6. Zakres dostępu, wynikający ze spełnienia przez urządzenie danych warunków polityki bezpieczeństwa powinien być egzekwowany przez mechanizm kwarantanny.</p> <p>7. Musi być możliwość łatwego, manualnego tworzenia białej listy adresów MAC, czyli listy urządzeń mogących bez żadnych ograniczeń ze strony NAC pracować w sieci.</p>
6.	Wymagania szczegółowe – mechanizm kwarantanny	<p>1. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenie, aby wyegzekwować ograniczenia dostępu do sieci, wynikające z polityki bezpieczeństwa</p> <p>2. Mechanizm kwarantanny powinien umożliwiać:</p> <ol style="list-style-type: none"> <li>całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym,</li> <li>częściowe blokowanie komunikacji urządzenia z otoczeniem sieciowym, w zakresie definiowanym przez administratora przez wskazanie adresów IP i portów, z którymi urządzenie może się komunikować</li> </ol> <p>3. Mechanizm kwarantanny powinien blokować komunikację urządzenia w czasie nie dłuższym niż 5 sekund od zaistnienia warunku, powodującego nałożenie kwarantanny</p> <p>4. Dla urządzeń zaufanych, czyli w polityce bezpieczeństwa spełniających kryteria pełnego dostępu do sieci, rozwiązanie nie powinno w żaden sposób przekierowywać ani blokować komunikacji wychodzącej z tych urządzeń</p> <p>5. Kwarantanna powinna być zdejmowana z urządzenia automatycznie, gdy spełni ono kryteria polityki bezpieczeństwa, pozwalające na pełny dostęp</p> <p>6. Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej, musi być niezależny od stosowanych w sieci przełączników, zarządzalnych bądź niezarządzalnych</p> <p>7. Awaria rozwiązania nie może powodować blokady komunikacji w sieci, tj. w przypadku awarii rozwiązania wszystkie urządzenia mają mieć pełny dostęp do sieci</p> <p>8. Rozwiązanie musi umożliwiać włączenie i wyłączenie mechanizmu kwarantanny (blokowania komunikacji) w każdej monitorowanej podsieci osobno</p>
7.	Wymagania szczegółowe – integracja z systemami zewnętrznymi	<p>1. Rozwiązanie musi umieć sprawdzić, czy urządzenia z systemem Windows są dołączone do domeny AD</p>

		<p>2. Rozwiązanie powinno umożliwiać sprawdzanie statusu oprogramowania antywirusowego, poprawek systemowych i firewalla bezpośrednio na zarządzanych stacjach roboczych Windows w domenie AD, w sposób bezagentowy, przy użyciu WMI.</p> <p>3. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym poprawkami Windows i sprawdzanie statusu zainstalowanych poprawek na zarządzanych urządzeniach z systemem Windows. Wymagana jest możliwość integracji co najmniej z systemami: Microsoft WSUS.</p> <p>4. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym agentami antywirusowymi i sprawdzanie statusu agentów AV zainstalowanych na zarządzanych urządzeniach (co najmniej, czy agent jest zainstalowany, aktywny i ma aktualne sygnatury wirusów). Wymagana jest możliwość integracji co najmniej z systemami: Bitdefender, Carbon Black, CrowdStrike, Cybereason, Eset, FireEye, McAfee, SentinelOne, Sophos, Symantec, TrendMicro, Webroot.</p> <p>5. Rozwiązanie musi umożliwiać wykorzystanie pozyskanych informacji, wymienionych w poprzedzających punktach 1-4, do definiowania polityki bezpieczeństwa.</p> <p>6. Rozwiązanie musi umieć odbierać alerty przysyłane za pomocą e-mail lub syslog z innych urządzeń bezpieczeństwa (np. firewalla) i na podstawie zawartych w nich informacji blokować wskazane podejrzanе urządzenie</p>
8.	Wymagania szczegółowe – rejestracja urządzeń zewnętrznych: pracowników, gości i konsultantów (Captive Portal)	<p>1. Rozwiązanie musi posiadać wbudowaną funkcję Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów. NAC musi przekierowywać ruch HTTP/S od nieznanych urządzeń do tego portalu.</p> <p>2. Captive Portal musi umożliwiać pracownikom rejestrowanie urządzeń prywatnych (BYOD) i wnioskowanie o dostęp do sieci w ograniczonym zakresie, zdefiniowanym przez administratora.</p> <p>3. Przy rejestracji przez pracowników ich prywatnych urządzeń, Captive Portal powinien umożliwiać użycie ich kont Active Directory</p> <p>4. Powinna istnieć możliwość ograniczenia ilości i rodzaju rejestrowanych przez pracownika prywatnych urządzeń</p> <p>5. Powinna być możliwość przypisania ograniczonego dostępu dla zarejestrowanych urządzeń prywatnych</p> <p>6. Captive Portal musi umożliwiać osobom niebędącym pracownikami (gościom lub konsultantom) wnioskowanie o ograniczony dostęp do sieci</p> <p>7. W przypadku rejestracji urządzeń gości powinna być możliwość rejestracji samodzielnie przez gościa oraz przez uprawnionego pracownika firmy</p> <p>8. Zarejestrowane urządzenia gości powinny automatycznie tracić przydzielony dostęp po upływie zdefiniowanego czasu</p> <p>9. Powinna istnieć możliwość ograniczenia ilości urządzeń rejestrowanych przez gościa</p> <p>10. Dla zarejestrowanych urządzeń gości powinna być możliwość ograniczenia, w jakich przedziałach czasu i z jakich podsieci będą one miały dostęp do sieci</p> <p>11. Dla urządzeń gości powinna być możliwość przypisania dostępu ograniczonego tylko do dostępu do internetu</p> <p>12. Dla urządzeń konsultantów powinna być możliwość przypisania dostępu ograniczonego do wybranych zasobów lokalnych</p> <p>13. Rozwiązanie musi umożliwiać zatwierdzenie dostępu dla zarejestrowanego urządzenia gościa i konsultanta drogą mailową. Osoba zatwierdzająca powinna otrzymać z systemu e-mail z wnioskiem o dostęp i udzielić go, odpowiadając na maila lub klikając przygotowany link w treści maila.</p> <p>14. Rozwiązanie musi przechowywać historyczne raporty dostępu do sieci użytkowników typu gość i konsultant</p> <p>15. Wygląd Captive Portal musi być edytowalny w zakresie co najmniej zmiany firmowego logo i kolorów oraz informacji, jakie we wniosku rejestracyjnym musi podać gość lub konsultant</p>

9.	Pozostałe wymagania	<p>1. Rozwiązanie powinno oferować uwierzytelnianie administratora za pomocą dodatkowego faktora, oprócz hasła (2FA).</p> <p>2. Rozwiązanie powinno oferować możliwość zainstalowania opcjonalnego agenta na zarządzanych stacjach roboczych (wymagane wsparcie dla Windows, Linux i MacOS), który przesyła do serwera zarządzającego NAC szczegółowe informacje na temat stacji roboczej, umożliwiając definiowanie na bazie tych informacji precyzyjnych polityk bezpieczeństwa.</p> <p>3. Rozwiązanie nie powinno pogarszać wydajności pracy przełączników i routerów, nie może wymagać współpracy z przełącznikami przez port mirroring czy port spanning.</p> <p>4. Rozwiązanie nie powinno pogarszać wydajność łącz WAN</p> <p>5. Rozwiązanie nie powinno pogarszać wydajności pracy monitorowanych urządzeń w sieci</p>
10.	Usługi	<p>Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, w wymienionym poniżej zakresie, przeprowadzoną przez wykwalifikowanego inżyniera, certyfikowanego przez producenta rozwiązania w siedzibie Zamawiającego:</p> <ul style="list-style-type: none"> <li>- instalacja i konfiguracja rozwiązania w maszynie wirtualnej na platformie Zamawiającego</li> <li>- szkolenie dla administratora rozwiązania</li> <li>- wsparcie w języku polskim w trybie 8x5 w dni robocze</li> <li>- kwartalny przegląd konfiguracji rozwiązania</li> </ul> <p>Wymaga się, aby dostawca przedstawił:</p> <ul style="list-style-type: none"> <li>- oświadczenie Producenta lub Autoryzowanego Dystrybutora Producenta o posiadaniu przez dostawcę kwalifikacji technicznych, niezbędnych do wykonania wdrożenia oferowanego rozwiązania i szkolenia należy załączyć do oferty</li> <li>- osobowy certyfikat inżynierski pracownika, która będzie wykonywał wdrożenie, należy załączyć do oferty</li> </ul>
11.	Wsparcie	<p>Wymaga się, aby dostawca zaoferował usługę zdalnego wsparcia w zakresie reagowania na raportowane przez NAC zdarzenia, przez okres minimum 24 miesięcy</p> <ul style="list-style-type: none"> <li>- w trybie ciągłym 24/7, z czasem reakcji 4 godziny, w zakresie:</li> <li>- odbieranie alertów mailowych wysyłanych przez NAC</li> <li>- bieżąca analiza raportowanych zdarzeń pod kątem istniejącego zagrożenia bezpieczeństwa sieci</li> <li>- natychmiastowe powiadamianie zespołu IT Zamawiającego w przypadku podejrzenia aktywnego zagrożenia i stwierdzenia konieczności szybkiej reakcji</li> <li>- merytoryczne wsparcie w procesie reagowania na raportowane przez NAC zagrożenia</li> <li>- okresowe sporządzanie podsumowań o zagrożeniach wykrytych z zraportowanych przez NAC (co miesiąc)</li> <li>- okresowe sporządzanie wykazu niezaufanych urządzeń, wykrytych przez NAC (co miesiąc)</li> <li>- okresowe weryfikowanie skuteczności monitorowania sieci przez NAC, poprzez celowe i kontrolowane wywołanie zdarzeń (raz na kwartał)</li> <li>- okresowe sprawdzanie dostępności aktualizacji i aktualizowanie oprogramowania NAC (co miesiąc)</li> </ul> <p>Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.</p>
12.	Testy penetracyjne infrastruktury wewnętrznej	<ul style="list-style-type: none"> <li>• Głównym celem testów bezpieczeństwa jest identyfikacja luk w zabezpieczeniach po wdrożeniu systemu NAC, w szczególności tych, które mogą mieć poważny wpływ na atrybuty bezpieczeństwa systemów i danych przetwarzanych przez systemy (poufność, integralność, dostępność).</li> <li>• Prace zostaną przeprowadzone zdalnie z wykorzystaniem połączenia VPN do zasobów Zamawiającego.</li> <li>• Prace będą wykonywane z jednego stałego adresu IP Wykonawcy.</li> <li>• Testy bezpieczeństwa muszą objąć wymagania weryfikacyjne określone w następujących dokumentach:</li> <li>• OWASP Web Security Testing Guide v4.2,</li> </ul>

- OWASP Top 10 2021,
- OWASP Application Security Verification Standard (ASVS) v4.0.3 (Level 2),
- Przebieg procesu testowania bezpieczeństwa aplikacji
- Próby zgromadzenia jak największej ilości dostępnych publicznie informacji na temat infrastruktury informatycznej
- Identyfikacja udostępnionych usług poprzez skanowanie portów TCP/UDP wraz z próbą uzyskania informacji o zainstalowanych wersjach oprogramowania wykorzystując techniki fingerprinting oraz banner grabbing
- Skanowanie podatności z wykorzystaniem automatycznych narzędzi
- Manualna identyfikacja podatności
- w oparciu o zgromadzone informacje
- o wersjach zainstalowanego na badanych urządzeniach oprogramowania w publicznych bazach (np. Bugtraq, CERT, OSVDB),
- Analiza mająca na celu weryfikację i eliminację potencjalnych fałszywych alarmów (false positives) oraz identyfikację krytycznych podatności,
- Próba odnalezienia kodu oprogramowania wykorzystującego daną podatność – tzw. exploit
- Kontrolowane próby wykorzystania stwierdzonych podatności
- Testy podatności są realizowane w oparciu o globalną metodykę, zgodną z opracowaniami OSSTMM (Open Source Security Testing Methodology Manual) LPT (License Penetration Testing) oraz najlepszymi praktykami w obszarze testów podatności.
- Testy penetracyjne infrastruktury prowadzone będą z wykorzystaniem automatycznych narzędzi służących do weryfikacji poziomu bezpieczeństwa infrastruktury oraz przy wykorzystaniu technik manualnych,
- Minimalne narzędzia jakie Wykonawca musi wykorzystać do przeprowadzenia testów zewnętrznych:
  - Nmap
  - Nessus Professional
  - OpenVAS
  - MetaSploit
  - Foca
  - Maltego
  - Skrypty i narzędzia autorskie w Kali linux,
  - Skrypty i narzędzia autorskie powershell do enumeracji infrastruktury Microsoft Windows,
- Zamawiający wymaga, aby Wykonawca posiada potencjał osobowy niezbędny do wykonania zamówienia. Zamawiający wymaga aby osoby testujące łącznie posiadały poniższe certyfikaty:
  - Offensive Security Certified Professional (OSCP);
  - Certified Information Systems Security Professional (CISSP);
  - Certified Security Analyst (ECSA);
  - Web Application Penetration Tester (eWPT);
  - Certified Professional Penetration Tester (eCPPT);
- o **Certyfikaty należy załączyć do oferty**

## 13. NAS TYP IV – 2 kpl.

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	Charakterystyka ogólna	Producent i model, oferowanego NAS. System NAS ma zapewnić bezpieczne przechowywane danych w środowisku informatycznym Starostwa, chroniąc przed utratą lub uszkodzeniem danych. Szybki dostęp do danych – zapewnia szybki odczyt i zapis danych, co jest kluczowe w przypadku systemu kopii bezpieczeństwa. Redundancja i kopie zapasowe – dzięki zdublowaniu urządzeń i systemom RAID zwiększy odporność na awarie. System do tworzenia kopii serwerów oraz stanowisk komputerowych
2.	Procesor	Wielordzeniowy procesor o architekturze 64-bitowej.
3.	Obudowa	Typu rack o wysokości maksymalnie 2U wraz z szynami przesuwными umożliwiającymi montaż w szafie rack w zestawie.
4.	Pamięć RAM	Minimum 16GB DDR4 ECC (2 x 8GB). Model pamięci musi znajdować się na oficjalnej liście zgodności producenta – nie zezwala się na stosowanie zamienników.
5.	Ilość obsługiwanych dysków	Minimum 12 dysków o maksymalnej pojemności nie mniejszej niż 18TB każdy, po podłączeniu modułów rozszerzających minimum 24 dyski.
6.	Zainstalowane dyski	10 dysków o pojemności 12TB każdy zgodnych z listą kompatybilności oferowanego serwera oraz charakteryzujących się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM, - gwarancja: minimum 36 miesięcy, - MTBF: minimum 1 milion, - możliwość aktualizacji oprogramowania dysku bezpośrednio z poziomu systemu operacyjnego serwera NAS.
7.	Interfejsy sieciowe	Minimum 2 porty 1GbE RJ-45. Minimum 1 port 10GbE RJ-45. Minimum 2 porty 10GbE SFP+. Obsługa agregacji łączy.
8.	Porty	Minimum 2 porty USB 3.2. Minimum 1 gniazdo rozszerzenia służące do podłączania jednostek rozszerzających.
9.	Wskaźniki LED	Status, HDD, zasilanie, LAN
10.	Obsługa RAID	Podstawowy, RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare.
11.	Funkcje RAID	Możliwość zwiększania pojemności poprzez wymianę dysków na większe. Migracja poziomu RAID w trybie online dla minimum RAID 1 i RAID 5.
12.	Szyfrowanie	Możliwość szyfrowania wybranych udziałów sieciowych.
13.	Protokoły	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP
14.	Usługi	1. Serwer VPN, Stacja monitoringu, Windows ACL, Integracja z Windows Active Directory, Firewall, Serwer plików, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Usługa DDNS, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki (min. 65 tys. w całym systemie), możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów.  2. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 7 lub nowszym według harmonogramu z możliwością zarządzania z poziomu centralnej konsoli dostępnej lokalnie oraz zdalnie, przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Dane z kopii



		<p>zapasowych muszą być redukowane poprzez globalną deduplikację po stronie miejsca przechowywania. Licencja musi umożliwiać podłączanie kolejnych komputerów do systemu kopii zapasowej bez limitu.</p> <p>3. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klaster obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora.</p>
15.	Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
16.	Język GUI	Polski
17.	Gwarancja i serwis	Minimum 12 miesięcy gwarancji Next Business Day On-site producenta na cały zestaw złożony z serwera, dysków i akcesoriów z gwarantowanym terminem naprawy sprzętu przez dedykowanego inżyniera w przypadku awarii sprzętowej na następny dzień roboczy z opcją pozostawienia uszkodzonego nośnika.
18.	Waga bez dysków	Maksymalnie 15 kg
19.	Typowy pobór mocy podczas pracy	Maksymalnie 130W
20.	Certyfikaty	CE, FCC
21.	System plików	Dyski wewnętrzne: BTRFS
22.	Szyfrowanie	Mechanizm szyfrowania sprzętowego
23.	Zasilacz	Redundantny zasilacz o mocy minimum 300W.
24.	Chłodzenie	Minimum 2 wentylatory z możliwością regulowania prędkości obrotowej oraz wymiany w urządzeniu podczas pracy.
25.	Dodatkowe Wsparcie techniczne	<p><b>Zakres dodatkowego wsparcia</b></p> <p>Wsparcie techniczne musi być świadczone przez wykwalifikowanych inżynierów Producenta oferowanego rozwiązania lub certyfikowanych inżynierów dystrybutora oferowanego rozwiązania na terenie Polski posiadającego autoryzację producenta od minimum 10 lat. Wymagane jest, aby osoby te posiadały odpowiednie kompetencje techniczne i doświadczenie w obsłudze oraz serwisowaniu urządzeń objętych niniejszą dostawą, co zapewni najwyższy poziom jakości usług oraz bezpieczeństwo danych Zamawiającego.</p> <ol style="list-style-type: none"> <li><b>Proaktywne monitorowanie infrastruktury</b> <ul style="list-style-type: none"> <li>Ciągłe monitorowanie pracy urządzeń, obejmujące: <ul style="list-style-type: none"> <li>Stan techniczny nośników danych, w tym parametry SMART, zużycie i temperaturę.</li> <li>Wykorzystanie zasobów systemowych, takich jak procesor, pamięć i przestrzeń dyskowa.</li> <li>Analizę logów systemowych pod kątem potencjalnych zagrożeń i anomalii.</li> </ul> </li> <li>Automatyczne powiadomienia o wykrytych problemach technicznych przesyłane do administratora Zamawiającego oraz zespołu wsparcia.</li> </ul> </li> <li><b>Kwartalne raportowanie stanu infrastruktury</b> <ul style="list-style-type: none"> <li>Przygotowywanie szczegółowych raportów technicznych zawierających: <ul style="list-style-type: none"> <li>Stan urządzeń, w tym status macierzy dyskowych oraz aktualną konfigurację systemową.</li> <li>Wykorzystanie zasobów i ich dynamikę w okresie sprawozdawczym.</li> <li>Informacje o liczbie zgłoszeń serwisowych, podejmowanych działaniach oraz ich wynikach.</li> <li>Rekomendacje dotyczące optymalizacji wydajności i planowania przyszłych działań.</li> </ul> </li> </ul> </li> </ol>

		<ul style="list-style-type: none"> <li>○ Raporty dostarczane w formie elektronicznej oraz omawiane podczas cyklicznych spotkań technicznych z przedstawicielami Zamawiającego.</li> </ul> <p><b>3. Reakcja serwisowa i wsparcie w sytuacjach krytycznych</b></p> <ul style="list-style-type: none"> <li>○ Gwarantowany czas reakcji na zgłoszenia: <ul style="list-style-type: none"> <li>▪ Krytyczne awarie: <b>maksymalnie 1 godzina</b> od zgłoszenia.</li> <li>▪ Problemy o wysokim priorytecie: <b>do 4 godzin roboczych</b>.</li> <li>▪ Problemy o niskim priorytecie: <b>do 1 dnia roboczego</b>.</li> </ul> </li> </ul> <p><b>4. Przeglądy techniczne i diagnostyka</b></p> <ul style="list-style-type: none"> <li>○ Realizacja kwartalnych przeglądów technicznych obejmujących: <ul style="list-style-type: none"> <li>▪ Weryfikację stanu nośników danych i macierzy RAID.</li> <li>▪ Aktualizację systemów operacyjnych oraz aplikacji zainstalowanych na urządzeniach.</li> <li>▪ Testowanie procedur odzyskiwania danych z kopii zapasowych.</li> <li>▪ Sprawdzanie konfiguracji systemów zabezpieczeń oraz logów w celu identyfikacji potencjalnych zagrożeń.</li> </ul> </li> <li>○ Każdy przegląd kończy się sporządzeniem szczegółowego raportu dla Zamawiającego wraz z rekomendacjami.</li> </ul> <p><b>5. Analiza ryzyk i doradztwo techniczne</b></p> <ul style="list-style-type: none"> <li>○ Regularne identyfikowanie potencjalnych zagrożeń dla działania urządzeń oraz opracowanie planów zapobiegawczych.</li> <li>○ Bieżąca analiza wydajności oraz analiza ryzyk związanych z przetwarzaniem danych.</li> <li>○ Proponowanie działań optymalizacyjnych, dostosowanych do zmieniających się potrzeb Zamawiającego.</li> </ul> <p><b>6. Wsparcie w integracji i optymalizacji infrastruktury</b></p> <ul style="list-style-type: none"> <li>○ Pomoc techniczna przy integracji urządzeń z istniejącą infrastrukturą sieciową i systemami informatycznymi Zamawiającego.</li> <li>○ Konfiguracja i utrzymanie mechanizmów zabezpieczeń danych, w tym systemów tworzenia kopii zapasowych oraz ich odtwarzania.</li> </ul> <p>Dostosowanie konfiguracji urządzeń do zmieniających się wymagań operacyjnych, zapewniające optymalne wykorzystanie zasobów</p> <p><b>Oferent winien przedłożyć dokumenty:</b>  Dokument potwierdzony przez Producenta lub Autoryzowanego Dystrybutora producenta o gotowości świadczenia na rzecz Zamawiającego wymaganego wsparcia (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).</p>
--	--	---

## 14. SYSTEM DO OCHRONY PRZED WYCIEKIEM DANYCH DLP – 50 LICENCJI

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	Architektura / budowa	<p>1.1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej <b>50</b> Klientów jednocześnie.</p> <p>1.2. Architektura / budowa:</p> <p>1.2.1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przysyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.</p> <p>1.2.1.1. Połączenie klient – serwer, Komunikacja odbywa się z wykorzystaniem TLS 1.3.</p> <p>1.2.1.2. Serwer i klient posiadają certyfikaty SSL (4096 bitowe).</p> <p>1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych,</p>

zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych).

1.2.3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach zgodnie ze specyfikacją opisaną poniżej.

1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.

1.2.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.

1.3. Konfiguracja Architektury:

1.3.1. Komponenty Klient, konsola administracyjna, serwer, baza danych muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu.

1.3.2. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja Klientów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie od producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją.

1.3.3. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, pakietów, pomoc i inne wbudowane bazy wiedzy.

1.3.4. Klient do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI.

1.3.5. Klient musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku \*.msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku \*.msi.

1.3.6. Klient musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej.

1.3.7. System zapewnia możliwość stworzenia instalatora (.exe) z wbudowanymi, zaszyfrowanymi poświadczeniami dla dowolnego konta. Funkcja ta umożliwia instalację usługi bezpośrednio na kontach użytkowników – zarówno lokalnych, jak i domenowych, korzystając z uprawnień zdefiniowanych dla instalatora w konsoli systemu.

1.3.8. Klient musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa).

1.3.9. System powinien umożliwiać generowanie unikatowego identyfikatora Klienta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków.

1.3.10. Klient musi mieć definiowalny priorytet pracy (ABOVE\_NORMAL, NORMAL, BELOW\_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów.

1.3.11. Klient musi wspierać wiele różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu Klienta.

1.3.12. System musi umożliwiać komunikację pomiędzy Klientami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.

1.3.13. System musi mieć możliwość współpracy komponentów Klient i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami Klientów.

		<p>1.4. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem.</p> <p>1.4.1. Automaty powinny realizować co najmniej:</p> <p>1.4.1.1. Usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nie przyrostowe, zmniejszanie bazy danych).</p> <p>1.4.2. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartości parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie</p>
2.	<b>Wymagania systemowe</b>	<p>2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).</p> <p>2.2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.</p> <p>2.2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2</p> <p>2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11.</p> <p>2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 8+.</p> <p>2.5. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).</p> <p>2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.</p>
3.	<b>Interfejsy</b>	<p>3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.</p> <p>3.1.1. Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.</p> <p>3.1.2. Import z Active Directory musi wspierać obsługę protokołów SSL oraz TLS.</p> <p>3.1.3. Import z Active Directory musi umożliwiać podanie więcej niż jednej domeny.</p> <p>3.2. System musi umożliwiać import użytkowników z zewnętrznego pliku CSV.</p> <p>3.3. System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switchy itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku *.xls, pliku *.xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane.</p> <p>3.4. System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS.</p> <p>3.5. System zapewnia integrację z modelem LLM.</p>
4.	<b>Funkcjonalności systemu</b>	<p>4.1. Funkcjonalność Klienta</p> <p>4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania Klienta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego).</p> <p>4.1.2. Klient musi mieć możliwość konfiguracji zakresu skanowania plików.</p>

4.1.3. Klient musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej, konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkownika, który go wyświetlił.

4.2. Funkcjonalność konsoli administracyjnej.

4.2.1. Konsola musi być w pełni polskojęzyczna.

4.2.2. Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie).

4.2.3. Konsola administracyjna musi posiadać dashboard – dashboard użytkownika, dashboard prezentujący parametry infrastruktury, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie.

4.2.4. Konsola administracyjna musi być wyposażona w panel zawierający graficzne widżety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi.

4.2.5. Dane na widżetach muszą być aktualizowane automatycznie.

4.2.6. System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widżety, ich konfigurację i kolejność).

4.2.7. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu.

4.2.8. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą mieć możliwość filtrowania kolumnowego.

4.2.9. System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.

4.2.10. Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu.

4.2.11. Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko).

4.2.12. Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja Klienta, stanu Klienta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera.

4.2.13. Konsola musi zawierać w sobie pełną dokumentację systemu.

4.3. Odczytywanie zainstalowanego oprogramowania

4.3.1. System powinien prezentować podgląd zainstalowanych systemów operacyjnych, pakietów oraz aplikacji na komputerach z informacjami o: nazwie, wersji, producencie, typie licencji.

4.4. Wzorce aplikacji i pakietów

4.4.1. System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 4 tys. wzorców aplikacji, 1,3 tys. Producentów.

4.4.2. System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania.

4.4.3. Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów.

4.4.4. System musi mieć możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera / komputerów wzorce mają być utworzone. Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu.

4.5. Inwentaryzacja sprzętu komputerowego

4.5.1. System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem).



4.5.2. System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language.

4.5.3. System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu).

4.5.4. System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania.

4.5.5. System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza począwszy od wskazanego miejsca w hierarchii kluczy rejestru.

4.5.6. System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu).

4.5.7. System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).

4.5.8. System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku.

4.5.9. System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu.

4.5.10. System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent).

4.5.11. System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne).

4.5.12. System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów.

4.5.13. System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik)

4.5.14. System umożliwia dodawanie notatek do każdej pozycji sprzętu.

4.5.15. System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).

4.5.15.1. System musi umożliwiać definiowanie typów serwisów

4.5.15.2. System musi umożliwiać definiowanie wartości serwisu

4.5.15.3. System musi umożliwiać definiowanie daty ważności serwisu oraz daty gwarancji

4.5.16. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium.

4.5.17. System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkownika, likwidacja).

4.6. Inwentaryzacja urządzeń podłączanych do komputera.

4.6.1. System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.)

4.6.2. System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika.

4.6.3. System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika).

4.7. Inwentaryzacja urządzeń sieciowych.

4.7.1. System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym IP/portcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać SNMP w wersji 1/2c/3.

4.7.2. Skaner SNMP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.

4.7.3. System musi zbierać informacje o jakości połączenia:

4.7.4. Czas odpowiedzi serwisów (usług) podawany w milisekundach:

4.7.4.1. Średni czas odpowiedzi.

4.7.4.2. Minimalny czas odpowiedzi.

4.7.4.3. Maksymalny czas odpowiedzi.

4.7.5. Ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat.

4.7.6. System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają Klienta.

4.7.6.1. Posiada niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci

4.7.6.2. Baza wzorców musi zawierać ponad 100 monitorowanych portów i usług.

4.7.6.3. System musi umożliwiać administratorowi definiowanie dodatkowych portów do monitorowania i przypisywanie do nich usług, a także modyfikowanie istniejących rekordów, obejmujących: port TCP, kategorię, nazwę usługi oraz nazwę skróconą.

4.7.7. System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci.

4.7.7.1. System musi umożliwiać generowanie map według dowolnych filtrów użytkownika.

4.8. Zdalna administracja komputerami

4.8.1. System ma automatycznie wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika.

4.8.1.1. System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu Windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania.

4.8.1.2. Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory Windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego.

4.8.1.3. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status).

4.8.1.4. System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, Windows PowerShell. System posiada co najmniej 70 predefiniowanych poleceń. System musi umożliwiać użytkownikom automatyczne definiowanie poleceń cmd/PowerShell. Funkcjonalność ta pozwala na wprowadzanie opisów zadanych czynności, a następnie, wykorzystując zaawansowane algorytmy AI, system automatycznie generuje adekwatne skrypty.

4.8.1.5. Zaawansowany Asystent AI do Przygotowywania Skryptów do precyzyjnego tworzenia szczegółowych skryptów

4.8.1.6. System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.).

4.8.1.7. System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)

4.8.1.8. System musi umożliwiać tworzenie zadań cyklicznych dla komputerów.

4.8.1.9. Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia,

pierwszy/drugi/trzeci/czwarty/ostatni  
poniedziałek/wtorek/środa/czwartek/piątek/sobota/niedziela/dzień wolny/dzień powszedni co n  
miesiący, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w  
pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni  
wybranego miesiąca, nowe zadanie n lat od wykonania.

4.8.1.10. System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n  
wystąpieniach, z końcem cyklu w określonej dacie.

4.8.2. System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania  
umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z  
identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro.

4.8.2.1. System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial  
Over LAN, zdalne włączanie, wyłączanie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie  
komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji.

4.8.2.2. System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro  
v.6).

4.8.3. System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki  
użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną  
instalację oprogramowania, poprawek i aktualizacji (service pack, patch).

4.8.3.1. System umożliwia zdalne połączenie do wielu komputerów jednocześnie i podgląd oraz  
operowanie na pulpitach tych komputerów w technologii Ultra VNC.

4.8.3.2. System musi umożliwiać uruchomienie do 6 sesji Ultra VNC na jednym ekranie.

4.8.3.3. System musi umożliwiać uruchomienie sesji Ultra VNC w trybie połączenia się do obecnie  
zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejęcia dostępu).

4.8.4. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.

4.8.5. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia  
pulpitu.

4.9. Wysyłanie wiadomości

4.9.1. Komunikator

4.9.1.1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę  
wiadomości pomiędzy użytkownikiem komputera z zainstalowanym Klientem a administratorem  
systemu.

4.9.1.2. Powinien zapewniać możliwość inicjowania czatu przez administratora.

4.9.1.3. Użytkownik powinien mieć opcję rozpoczęcia rozmowy za pomocą ikony na pasku zadań,  
która automatycznie uruchamia się zgodnie z konfiguracją Klienta.

4.9.1.4. System musi przechowywać historię konwersacji.

4.9.1.5. Powinien informować administratora poprzez powiadomienie w konsoli systemowej o  
nowych wiadomościach od użytkowników.

4.9.2. Wiadomość Jednorazowa:

4.9.2.1. System powinien umożliwiać wysyłanie jednorazowych wiadomości w trybie  
natychmiastowym jako ALERT.

4.9.2.2. Musi oferować możliwość wysłania wiadomości z opcją odłożenia na później (na 10 minut, 1,  
2, 4 godziny) dla późniejszego odczytu.

4.9.2.3. Powinien zapewniać historię wysyłania i odbierania wiadomości przez użytkowników, z  
możliwością edycji treści w edytorze HTML.

4.9.2.4. Wiadomość powinna być dostępna do wysłania do określonej grupy, wybranych komputerów  
lub użytkowników.

4.9.2.5. System musi umożliwiać konfigurację czasu wygaśnięcia wiadomości.

4.9.3. Wiadomości Cykliczne:

4.9.3.1. Powinien pozwalać na tworzenie szablonów wiadomości do regularnego użytku.

4.9.3.2. Musi zapewniać funkcję odłożenia wysłania wiadomości dla późniejszego odczytu, z  
możliwością edycji treści w edytorze HTML.

4.9.3.3. System powinien rejestrować historię wysyłania i odczytywania wiadomości przez  
użytkowników.

4.9.3.4. Powinien umożliwiać wysłanie wiadomości do zdefiniowanej grupy, wybranych komputerów lub użytkowników.

4.9.3.5. Musi oferować opcję konfiguracji terminu, po którym wiadomość wygaśnie.

4.9.4. System szkolenia pracowników za pomocą wiadomości.

4.9.4.1. System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów.

4.9.4.2. System musi posiadać predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa”, „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa”, „Postępowanie w przypadku naruszenia tajemnicy”, „Udostępnienie informacji stanowiących tajemnicę”.

4.9.4.3. Formatowanie treści musi być zgodne z HTML.

4.9.4.4. System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych).

4.9.4.5. System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców.

4.9.4.6. Użytkownik otrzymujący wiadomość musi być powiadamiany wizualnie i dźwiękowo o otrzymaniu nowej wiadomości.

4.9.4.7. Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.

4.9.4.8. System musi udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników.

4.9.4.9. System musi generować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem).

4.10. Repozytorium CMDDB

4.10.1.1. System musi posiadać wbudowaną centralną bazę systemu umożliwiającą import i eksport niektórych danych zarówno poprzez API jak też za pomocą wbudowanego import/eksportu.

4.11. Worktime manager

4.11.1. System musi być wyposażony w zestaw statystycznych danych o pracy użytkownika i zdefiniowanych grup użytkowników.

4.11.2. System musi umożliwiać definiowanie dowolnej ilości grup użytkowników przypisanych do dowolnej ilości przełożonych.

4.11.3. System musi umożliwić wyświetlanie informacji o użytkowniku pobranych z Active Directory. Informacje powinny być aktualizowane zgodnie z harmonogramem połączenia z domeną.

4.12. Zarządzanie politykami bezpieczeństwa.

4.12.1. System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez bieżące (w czasie rzeczywistym) monitorowanie działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa oraz reguł ich opisujących.

4.12.2. System musi zapewniać automatyczne uruchamianie ochrony zasobów w czasie rzeczywistym zgodnie ze zdefiniowanymi politykami.

4.12.3. System musi zapewniać ciągłą ochronę danych niezależnie od położenia komputera (w sieci lokalnej, sieci VPN, poza siecią).

4.12.4. System musi na bieżąco monitorować i chronić za pomocą odpowiednio zdefiniowanych polityk i reguł dane w ruchu, dane w spoczynku oraz dane w użyciu.

4.12.5. Przez dane w spoczynku rozumie się dane, które nie są (ale mogą być) w ruchu lub w użyciu, wymagają inwentaryzacji i zabezpieczenia.

4.12.6. Przez dane w użyciu należy rozumieć dane, które są aktywnie przetwarzane przez dowolną aplikację i/lub punkt końcowy (komputer). Przykłady danych w użyciu: edycja dokumentu MS Word, Excel, PowerPoint, edycja pliku tekstowego CSV, TXT, tworzenie pliku, przechwytywanie ekranu (screenshot), kopiowanie / wklejanie danych.

4.12.7. Przez dane w ruchu należy rozumieć dane, które są przesyłane, np. kopiowanie danych (plików) z dysku sieciowego na nośnik USB, kopiowanie danych (plików) z komputera na komputer, przesyłanie danych e-mailem w treści lub w postaci załącznika, pobieranie danych z serwera FTP, przesyłanie danych za pomocą komunikatora.

4.12.8. Obiekty docelowe reguł muszą być definiowalne za pomocą parametrów takich jak: nazwa komputera, adres IP, unikatowy identyfikator agenta, status połączenia do systemu (online/offline), zainstalowany system operacyjny, nazwę zalogowanego użytkownika, model komputera, producent komputera, dostawca komputera, budżet, z którego zakupiony został komputer, strukturę organizacyjną

4.12.9. Przy definiowaniu obiektów docelowych dla reguł DLP można korzystać ze znaków wieloznacznych.

4.12.10. System musi posiadać funkcjonalności monitorowania, blokowania, powiadomieniu użytkownika o wystąpieniu naruszenia zdefiniowanej polityki oraz pełnego logowania zdarzeń dotyczących polityki dla celów administracyjnych (powiadomienie administratora systemu).

4.12.11. System musi mieć możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP.

4.12.12. System musi mieć możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji.

4.12.13. Nowy komputer zgłaszający się do systemu po raz pierwszy musi bez dodatkowej ingerencji administratora automatycznie pobrać oraz wdrożyć (uruchomić) przeznaczoną dla niego politykę.

4.12.14. System musi mieć możliwość określenia ram czasowych działania danej reguły.

4.12.15. System musi dysponować mechanizmami dostępu do plików na poziomie jądra systemu operacyjnego MS Windows (32-bit i 64-bit), co uniemożliwia obejście zabezpieczeń nawet osobie z uprawnieniami administratora na poziomie systemu operacyjnego.

4.13. System musi w pełni wspierać następujące polityki ochrony danych:

4.13.1. Zdefiniowanie schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione

4.13.2. Wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku).

### 5. Kontrola i ochrona urządzeń (KU)

5.1. Blokowanie dostępu do wybranych typów urządzeń od strony sprzętowej. Wsparcie dla CD-ROM, portów USB, kart sieciowych, GPS, kart graficznych, modemów, klawiatur, czytników kart, drukarek, urządzeń Bluetooth i innych, monitorowanie podłączanych urządzeń. (DEVICE)

5.2. Blokowanie dostępu do urządzeń USB, tworzenie czarnych list urządzeń, monitorowane podłączanych urządzeń USB. (REMOVABLE DEVICE)

5.3. Zarządzanie dostępem do sieci społecznościowych, serwisów informacyjnych, blogów, bibliotek, forów dyskusyjnych oraz dowolnych stron www. (WEB)

5.3.1. Blokowanie sieci ze względu na zdefiniowany typ i maskę sieci WIFI. Polityka musi zapewniać blokowanie dostępu do sieci zarówno otwartych jak i zabezpieczonych. (WLAN)

5.4. Umożliwienie powiadamianie o przekroczeniu dozwolonego czasu pracy komputera. (WORKING TIME)

### 6. Ochrona danych w użyciu (DU)

6.1. Podjęcie działania w momencie uruchomienia określonego procesu. (PROCESS)

6.2. Podjęcie działań monitorowania i blokowania operacji w momencie próby kopiowania tekstu, zdjęcia czy ścieżki plików do schowka. (CLIPBOARD)

6.3. Monitorowanie wykonywanych zrzutów ekranu, blokowanie możliwości zapisania i wykorzystania zrzutów ekranu. (PRINTSCREEN)

6.4. Przechwytywanie zrzutów ekranu z komputerów użytkowników wyzwalany akcją użytkownika lub na życzenie administratora zgodnie z wcześniej ustawionym interwałem czasowym. (SCREEN MONITORING)

### 7. Ochrona danych w ruchu (DR)

7.1. Monitorowanie danych przesyłanych za pomocą poczty e-mail oraz blokowanie przesyłania plików określonych typów. (E-MAIL)



7.2. Monitorowanie danych przesyłanych do chmury oraz blokowanie synchronizacji plików określonych typów z wybraną chmurą. (CLOUD STORAGE)

7.3. Monitorowania i blokowania operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach. (FILE MOVE COPY)

#### 8. Klasyfikacja i ochrona dokumentów (KD)

8.1. Oznaczanie na dowolnym komputerze (znakowanie przez agenta) określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami. (FINGERPRINT)

8.2. Znakowanie określonych plików przechowywanych w zasobach serwerów lub udostępnionych zasobach (np. samodzielna macierz dyskowa) wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami, z wykorzystaniem harmonogramu. (SCHEDULED TAGGING)

#### 9. Raportowanie i eksport danych

9.1. System musi umożliwiać wyeksportowanie wybranych lub wszystkich danych do formatu .xls, .xlsx, .csv, .calc (OpenOffice), .html, .mht, .xml, .jpeg, .png, .gif, .bmp.

9.2. System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów, przy czym generowanie raportu musi odbywać się po stronie serwera www.

9.3. System powinien umożliwiać eksport danych z raportu do formatów: pdf, xls, doc, rtf.

9.4. System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).

9.5. System musi istnieć możliwość tworzenia i dodawania własnych raportów przez użytkownika.

#### 10. Bezpieczeństwo

10.1. System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.

10.1.1. Uwierzytelnianie do systemu musi być realizowane:

10.1.1.1. z wykorzystaniem imiennego konta użytkownika i hasła,

10.1.1.2. z wykorzystaniem imiennego konta administratorów aplikacji i hasła,

10.1.1.3. za pośrednictwem uwierzytelniania poprzez Active Directory,

10.1.1.4. za pośrednictwem uwierzytelniania poprzez CAS,

10.1.2. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej.

10.1.3. Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków).

10.1.4. System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie (MFA).

10.1.4.1. Uwierzytelnianie z wykorzystaniem obrazu wideo.

10.1.4.2. Uwierzytelnianie z jednorazowym kodem wysyłanym na e-mail użytkownika.

10.1.4.3. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe wraz z hasłem, które umożliwia jednoczesną pracę wielu użytkownikom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory/LDAP.

10.1.5. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania w oparciu o RSA 512/1024/RSA 2048 bit, ECDSA 192/256 bit, DES/3DES, AES 128/192/256 bit, SHA-1 / SHA-256.

10.1.5.1. Wykorzystywane klucze muszą posiadać wsparcie dla systemów Windows 7/8.1/10 i Windows Server 2012/2016/2019.

10.1.6. System musi umożliwiać blokadę dostępu po nieudanej próbie zalogowania się do systemu. Ponadto, system powinien oferować:

10.1.6.1. Podgląd wszystkich zablokowanych administratorów systemu, w tym informacje o typie, elemencie, czasie trwania blokady [s] oraz o ostatniej aktywności.

10.1.6.2. Możliwość odblokowania zablokowanego administratora systemu z poziomu konsoli administracyjnej przez osobę uprawnioną.

10.1.7. Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport.

10.1.8. System musi oferować możliwość podglądu wszystkich aktualnie otwartych sesji administratorów w konsoli administracyjnej, obejmując takie informacje jak: data utworzenia sesji, login, IP oraz SID.

10.1.8.1. Dodatkowo, system powinien umożliwiać wyszukiwanie zalogowanych administratorów po nazwie.

10.1.9. System musi udostępniać historię działań wybranych użytkowników/administratorów w zakresie, adresy URL i nagłówki http.

10.1.10. System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy Klientami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera.

10.1.11. System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nie przyrostowej oraz udostępniać informacje o rezultacie wykonania kopii.

10.1.12. System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych.

10.1.13. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy).

10.1.14. System musi być wyposażony w mechanizmy powtórznego załadowania danych historycznych pochodzących od Klientów.

10.1.15. System musi zapewniać:

10.1.15.1. Pełne logowanie błędów w celu weryfikowania nieprawidłowości.

10.1.15.2. Przechowywanie logów systemowych.

10.1.15.3. Przechowywanie logów bezpieczeństwa.

10.1.15.4. Przechowywanie logów aktywności użytkowników i administratorów.

10.1.15.5. Pobieranie logów z Klientów z poziomu konsoli administracyjnej.

10.1.15.6. Możliwość eksportu logów.

10.1.15.7. Definiowanie maksymalnego czasu przechowywania plików log.

10.1.15.8. System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.

10.1.15.9. Definiowanie ścieżki do kopii zapasowej

10.1.15.10. Definiowanie ścieżki do importu danych

10.1.15.11. Definiowanie ścieżki do zapisu raportów

10.1.15.12. Definiowanie serwera do importu danych

11. Wsparcie i pomoc

11.1.1. System musi posiadać dokumentację w postaci min. 5 filmów instruktażowych/nagrań z webinarium w języku polskim.

11.1.2. System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim.

11.1.3. Pomoc techniczna

11.1.3.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.

11.1.3.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.

11.1.3.3. Czas trwania usługi SLA wynosi 12 miesięcy od dnia zakupu.

11.1.3.4. Usługi Utrzymania Oprogramowania obejmują:

11.1.3.4.1. asystę techniczną,

11.1.3.4.2. świadczenie usług SLA, w ramach, których realizowana jest:

11.1.3.4.2.1. obsługa zgłoszeń w zakresie:

11.1.3.4.2.1.1. reakcja na zgłoszenia błędów w określonym czasie reakcji;

11.1.3.4.2.1.2. dokonywanie analizy przyczyn błędów;

11.1.3.4.2.1.3. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich;

11.1.3.4.2.1.4. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie infrastruktury zamawiającego;  
 11.1.3.4.2.1.5. usuwania błędów w czasie naprawy;  
 11.1.3.4.2.1.6. usuwania błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich – po udostępnieniu odpowiedniej aktualizacji przez producenta tego oprogramowania oraz jej uzyskaniu – w czasie naprawy;  
 11.1.3.5. zapewnienia dostępności Oprogramowania.

## 15. ZAKUP NOWYCH MODUŁÓW DO SYSTEMU INWENTARYZACJI AKTYWÓW – 50 LICENCJI

LP	Parametr	Wymagania minimalne
1	Upgrade do wersji eAuditor V9 AI	<p>Przedmiotem zamówienia jest rozszerzenie posiadanego przez Zamawiającego systemu eAuditor o dodatkowe moduły funkcjonalne oraz wykupienie wsparcia serwisowego obejmującego okres minimum 12 m-cy r. W ramach niniejszego zamówienia przewiduje się:</p> <ul style="list-style-type: none"> <li>-aktualizację do wersji eAuditor V9 Standard AI,</li> <li>- zakup i wdrożenie modułów WebRTC oraz Patch Management (Zdalne zarządzanie poprawkami i aktualizacjami).</li> </ul> <p>Wdrożenie ma na celu zapewnienie bieżącej, zautomatyzowanej kontroli nad infrastrukturą IT w zakresie komunikacji z użytkownikami i zarządzania aktualizacjami systemów operacyjnych oraz aplikacji, z uwzględnieniem wymagań określonych w programie „Cyberbezpieczny Samorząd”</p> <p>System musi zostać zaktualizowany do wersji eAuditor V9 Standard AI z zachowaniem wszystkich dotychczasowych danych i konfiguracji. Wersja ta powinna wspierać nowoczesne mechanizmy analityczne oraz funkcje wspomagane przez sztuczną inteligencję w zakresie zarządzania infrastrukturą IT. System musi umożliwiać pracę dla co najmniej 50 stanowisk.</p>
2	Moduł WebRTC	System musi zapewniać zdalne zarządzanie komputerami przy użyciu technologii WEBRTC, umożliwiając jednocześnie połączenia z wieloma urządzeniami, przejęcie kontroli nad pulpitemi, zarządzanie plikami i aplikacjami, instalowanie aktualizacji, nagrywanie sesji oraz ich podgląd. Musi być możliwe uruchomienie do 12 sesji równoległych na jednym ekranie z pełną konfiguracją połączeń.
3	Moduł Patch Management	System musi posiadać funkcjonalność zdalnego zarządzania poprawkami i aktualizacjami, umożliwiającą wykrywanie nieaktualnych aplikacji, planowanie instalacji aktualizacji, zarządzanie poprawkami systemowymi i aplikacyjnymi oraz generowanie raportów zgodności. Moduł powinien wspierać harmonogramowanie zadań i automatyzację wdrażania poprawek na urządzeniach końcowych.
4	Warunki równoważności	<p>Zamawiający dopuszcza dostawę oprogramowania równoważnego. Przez równoważność oprogramowania należy rozumieć spełnienie następujących wymagań</p> <ol style="list-style-type: none"> <li>oferowane oprogramowanie musi spełniać wymagania określone w punkcie C zawierającym specyfikację wymagań funkcjonalnych,</li> <li>wykonawca wdroży oprogramowanie równoważne w terminie wskazanym w ofercie, przy czym okres od deinstalacji dotychczas funkcjonującego oprogramowania do wdrożenia zaproponowanego oprogramowania równoważnego nie może być dłuższy niż 3 dni robocze. Czynności wykonywane będą w godzinach pracy zamawiającego tj. od godz. 7:30 do godz. 15:30, od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy,</li> <li>wykonawca przeszkoli personel techniczny w zakresie używania, zarządzania oraz administrowania programem,</li> <li>wykonawca przygotuje i przekaze zamawiającemu wersję elektroniczną instrukcji obsługi interfejsu użytkownika oprogramowania zainstalowanego na komputerze,</li> <li>wykonawca dokona zainstalowania oprogramowania na komputerach w liczbie zgodnej z liczbą wymaganych licencji.</li> </ol> <p>B. Wymagane minimalne parametry techniczne</p> <p><b>B.1. Abonament serwisowy systemu e-Auditor wraz z dodatkowymi funkcjonalnościami</b></p>

**1. Architektura / budowa**

- 1.1. System musi umożliwić bezproblemową i stabilną obsługę 50 Klientów jednocześnie.
- 1.2. Architektura / budowa:
  - 1.2.1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przysyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
  - 1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).
  - 1.2.3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.
  - 1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.
  - 1.2.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.
- 1.3. Konfiguracja Architektury:
  - 1.3.1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.
  - 1.3.2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.

**2. Wymagania systemowe**

- 2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Edge, FireFox, Chrome, Opera).
- 2.2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.
  - 2.2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2
- 2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11.
- 2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9.
- 2.5. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych, bezpłatnej (np. Microsoft SQL Server Express Edition).
- 2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

**3. Interfejsy**

- 3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
- 3.2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL
- 3.3. System zapewnia integrację z modelem LLM.

**4. Funkcjonalności systemu zarządzania infrastrukturą IT**

- 4.1. Funkcjonalność Klienta
  - 4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkownikowi.
- 4.2. Funkcjonalność konsoli administracyjnej.
  - 4.2.1. Konsola administracyjna musi być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie.
  - 4.2.2. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych

- ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.
- 4.2.3. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.
- 4.3. Funkcjonalność panelu pracownika
- 4.3.1. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.
- 4.4. Zarządzanie licencjami
- 4.4.1. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.
- 4.5. Wzorce aplikacji i pakietów
- 4.5.1. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.
- 4.6. Inwentaryzacja sprzętu komputerowego i urządzeń.
- 4.6.1. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń.
- 4.7. Inwentaryzacja urządzeń sieciowych.
- 4.7.1. System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.
- 4.8. Inwentaryzacja sprzętu.
- 4.8.1. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.
- 4.9. Ochrona danych (DLP)
- 4.9.1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwoleńmi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.
- 4.10. Szyfrowanie dysków wewnętrznych oraz zewnętrznych
- 4.10.1. System musi obsługiwać kompleksowe szyfrowanie dysków wewnętrznych i zewnętrznych USB, z wykorzystaniem BitLocker i różnych metod szyfrowania, takich jak XTS\_AES\_256 i AES\_128. Musi umożliwiać zdalne zarządzanie procesem szyfrowania/desyfrowania, w tym masowe operacje na partycjach systemowych i niesystemowych, zarówno lokalnie, jak i zdalnie (poza NATem). Klucze szyfrujące są przechowywane i chronione w konsoli administracyjnej, dostępne tylko po uwierzytelnieniu administratora. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika i nie może być przez niego przerwany, z wyjątkiem stanów hibernacji i wyłączenia systemu, po których jest automatycznie kontynuowany.
- 4.11. Zdalna administracja komputerami
- 4.11.1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za



pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.

4.12. System musi umożliwiać zdalne w technologii WEBRTC.

4.12.1. System musi zapewniać zdalne zarządzanie komputerami przy użyciu technologii WEBRTC, umożliwiając jednocześnie połączenia z wieloma urządzeniami. Powinien oferować funkcje takie jak przejęcie kontroli nad pulpitemi, zarządzanie plikami, uruchamianie i zarządzanie aplikacjami oraz instalowanie oprogramowania i aktualizacji. System powinien umożliwiać konfigurację połączeń WEBRTC, w tym instalację i konfigurację odpowiednich serwerów i portów. Dodatkowo, system powinien obsługiwać różne tryby przejęcia sesji, włączając opcje z lub bez zgody użytkownika, a także umożliwiać nagrywanie i zarządzanie sesjami połączeń, w tym wykonywanie zrzutów ekranu i nagrywanie sesji. System powinien również wspierać różnorodne konfiguracje wyświetlania i jakości sesji, a także umożliwiać uruchomienie do 12 sesji na jednym ekranie.

4.13. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.

4.14. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.

4.15. Zdalna instalacja

4.15.1. System musi umożliwiać zdalną instalację pakietów MSI i plików .exe, korzystając z Windows Management Instrumentation (WMI) oraz usługi Klient bez dodatkowych poświadczeń, wykorzystując lokalne i sieciowe repozytoria. Powinien obsługiwać tworzenie repozytorium instalatorów z możliwością dodawania aplikacji, zarządzania wersjami oraz kategoryzacji. System musi również umożliwiać tworzenie grup instalacyjnych, definiowanie schematów instalacyjnych i automatyzację procesu instalacji na nowych urządzeniach. Powinien zawierać kiosk aplikacji umożliwiający użytkownikom samodzielną instalację aplikacji oraz rejestrować i raportować wszystkie procesy instalacji, umożliwiając również ich przerwanie.

4.16. Zdalne Zarządzanie Zaporą (Firewall)

4.16.1. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.

4.17. Automatyzacja

4.17.1. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.

4.18. Zarządzanie magazynem IT

4.18.1. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.

4.19. Repozytorium

4.19.1. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.

4.20. Kody kreskowe

4.20.1. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.

4.21. Wysyłanie wiadomości

- 4.21.1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między administratorem a użytkownikami systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.
- 4.22. System musi posiadać możliwość eksportu / importu treści.
- 4.23. Monitorowanie drukarek sieciowych i wydruków
- 4.23.1. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.
- 4.24. Monitorowanie stron www
- 4.24.1. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.
- 4.25. Monitorowanie serwerów WWW
- 4.25.1. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.
- 4.26. Monitorowanie dziennika zdarzeń
- 4.26.1. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.
- 4.27. System musi umożliwiać monitorowanie komunikatów Syslog.
- 4.28. Monitorowanie pracy komputerów
- 4.28.1. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.
- 4.29. Monitorowanie uprawnień ACL
- 4.29.1. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizację danych i filtry do zarządzania informacjami.
- 4.30. Monitorowanie sensorów
- 4.30.1. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.
- 4.31. Repozytorium CMDB
- 4.31.1. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.
- 4.32. Worktime manager
- 4.32.1. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostępnienia w panelu pracownika.
- 4.33. Raportowanie i eksport danych
- 4.33.1. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz

		<p>zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.</p> <p>4.34. System musi zapewnić interfejs API.</p> <p>4.34.1. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.</p> <p>4.35. Powiadomienia</p> <p>4.35.1. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji.</p> <p>4.36. Bezpieczeństwo</p> <p>4.36.1. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.</p> <p>5. Wsparcie i pomoc</p> <p>5.1.1. Pomoc techniczna</p> <p>5.1.1.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.</p> <p>5.1.1.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.</p> <p>5.1.1.3. Czas trwania usługi SLA wynosi 12 m-cy od dnia zakupu .</p>
--	--	--

## 16. UTM TYP II

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	<b>Wymagania Ogólne</b>	<p>System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> <li>• Firewall.</li> <li>• Ochrony w warstwie aplikacji.</li> <li>• Protokołów routingu dynamicznego.</li> </ul>
2.	<b>Redundancja, monitoring i wykrywanie awarii</b>	<ol style="list-style-type: none"> <li>1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.</li> <li>2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</li> <li>3. Monitoring stanu realizowanych połączeń VPN.</li> </ol>

		4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
3.	<b>Interfejsy, Dysk, Zasilanie:</b>	<ol style="list-style-type: none"> <li>1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:</li> <li>2. 10 portami Gigabit Ethernet RJ-45.</li> <li>3. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.</li> <li>4. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.</li> <li>5. System jest wyposażony w zasilanie AC.</li> </ol>
4.	<b>Parametry wydajnościowe:</b>	<ol style="list-style-type: none"> <li>1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 100 tys. nowych połączeń na sekundę.</li> <li>2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.</li> <li>3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.5 Gbps.</li> <li>4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 7 Gbps.</li> <li>5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 2.4 Gbps.</li> <li>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 1.3 Gbps.</li> <li>7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1.4 Gbps.</li> </ol>
5.	<b>Funkcje Systemu Bezpieczeństwa:</b>	<p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none"> <li>1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.</li> <li>2. Kontrola Aplikacji.</li> <li>3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN .</li> <li>4. Ochrona przed malware.</li> <li>5. Ochrona przed atakami - Intrusion Prevention System.</li> <li>6. Kontrola stron WWW.</li> <li>7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.</li> <li>8. Zarządzanie pasmem (QoS, Traffic shaping).</li> <li>9. 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.</li> </ol>

		<p>10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.</p> <p>11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.</p> <p>12. 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).</p>
6.	<b>Polityki, Firewall</b>	<ol style="list-style-type: none"> <li>1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</li> <li>2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: <ul style="list-style-type: none"> <li>• Translację jeden do jeden oraz jeden do wielu.</li> <li>• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.</li> </ul> </li> <li>3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</li> <li>4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.</li> <li>5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</li> <li>6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</li> <li>7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. <ul style="list-style-type: none"> <li>• Amazon Web Services (AWS).</li> <li>• Microsoft Azure.</li> <li>• Cisco ACI.</li> <li>• Google Cloud Platform (GCP).</li> <li>• OpenStack.</li> <li>• VMware NSX.</li> <li>• Kubernetes.</li> </ul> </li> </ol>
7.	<b>Połączenia VPN</b>	<ol style="list-style-type: none"> <li>1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: <ul style="list-style-type: none"> <li>• Wsparcie dla IKE v1 oraz v2.</li> <li>• Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).</li> <li>• Obsługę protokołu Diffie-Hellman grup 19, 20.</li> <li>• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.</li> <li>• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.</li> <li>• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</li> <li>• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.</li> </ul> </li> </ol>



		<ul style="list-style-type: none"> <li>• Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.</li> <li>• Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.</li> <li>• Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.</li> <li>• Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.</li> <li>• Mechanizm „Split tunneling” dla połączeń Client-to-Site.</li> </ul> <p>2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.</p>
8.	<b>Routing i obsługa łączy WAN</b>	<p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <ol style="list-style-type: none"> <li>1. Routingu statycznego.</li> <li>2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).</li> <li>3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.</li> <li>4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.</li> <li>5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.</li> <li>6. BFD (Bidirectional Forwarding Detection).</li> <li>7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.</li> </ol>
9.	<b>Funkcje SD-WAN</b>	<ol style="list-style-type: none"> <li>1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</li> <li>2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</li> </ol>
10.	<b>Zarządzanie pasmem</b>	<ol style="list-style-type: none"> <li>1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</li> <li>2. System daje możliwość określania pasma dla poszczególnych aplikacji.</li> <li>3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</li> <li>4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.</li> </ol>
11.	<b>Ochrona przed malware</b>	<ol style="list-style-type: none"> <li>1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</li> <li>2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</li> <li>3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.</li> <li>4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</li> </ol>

		<ol style="list-style-type: none"> <li>System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</li> <li>Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</li> <li>System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.</li> <li>Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</li> <li>Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</li> </ol>
12.	Ochrona przed atakami	<ol style="list-style-type: none"> <li>Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</li> <li>System chroni przed atakami na aplikacje pracujące na niestandardowych portach.</li> <li>Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</li> <li>Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.</li> <li>System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</li> <li>Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</li> <li>Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.</li> <li>Wykrywanie i blokowanie komunikacji C&amp;C do sieci botnet.</li> <li>Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.</li> </ol>
13.	Kontrola aplikacji	<ol style="list-style-type: none"> <li>Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</li> <li>Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</li> <li>Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</li> <li>Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</li> <li>Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</li> <li>Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 21).</li> <li>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).</li> </ol>
14.	Kontrola WWW	<ol style="list-style-type: none"> <li>Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</li> </ol>

		<ol style="list-style-type: none"> <li>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.</li> <li>3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.</li> <li>4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</li> <li>5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</li> <li>6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</li> <li>7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</li> <li>8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</li> <li>9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji</li> </ol>
15.	Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none"> <li>1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: <ul style="list-style-type: none"> <li>• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</li> <li>• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</li> <li>• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</li> </ul> </li> <li>2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</li> <li>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.</li> <li>4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</li> </ol>
16.	Zarządzanie	<ol style="list-style-type: none"> <li>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.</li> <li>2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</li> <li>3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.</li> <li>4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</li> <li>5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</li> <li>6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</li> <li>7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</li> <li>8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</li> </ol>

		9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
17.	Logowanie	<ol style="list-style-type: none"> <li>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.</li> <li>2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowaniem ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</li> <li>3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</li> <li>4. Możliwość włączenia logowania per reguła w polityce firewall.</li> <li>5. System zapewnia możliwość logowania do serwera SYSLOG.</li> <li>6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</li> </ol>
18.	Testy wydajnościowe oraz funkcjonalne	1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni)
19.	Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.
20.	Gwarancja oraz wsparcie	<p>System jest objęty serwisem gwarancyjnym producenta przez okres [12] miesiące polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie zamawiającego, realizowana przez producenta lub autoryzowanego dystrybutora w języku polskim przez okres wymaganej gwarancji.</p> <p>Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji.</p> <p>Do zamawianego sprzętu Wykonawca zapewni usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:</p> <ul style="list-style-type: none"> <li>obsługa procesu RMA u producenta,</li> <li>zdalna pomoc w skonfigurowaniu urządzenia do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producenta,</li> <li>jednorazowa podstawowa konfiguracja platformy realizowana przez inżyniera z najwyższym dostępnym poziomem certyfikacji technicznej producenta,</li> <li>dostęp do szkolenia wideo prezentującego najlepsze praktyki współpracy z suportem producenta systemu realizującego funkcję Firewall.</li> </ul>

Dostęp do usługi powinien być świadczony przez dedykowaną infolinię (należy podać numer telefonu) oraz przez dedykowany moduł internetowy (należy podać adres).

Usługa ta ma być świadczona przez podmiot posiadający certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.

Do oferty wymagane jest załączenie dokumentu sygnowanego przez Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).

Certyfikat ISO 9001 podmiotu serwisującego.

## 17. MINIMALNE WYMAGANIA DOTYCZĄCE WDROŻEŃ I SZKOLEŃ

### A WDROŻENIE SERWERA I BIBLIOTEKI TAŚMOWEJ

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	Analiza Przedwdrożeńiowa	<ul style="list-style-type: none"> <li>- Audyt Infrastruktury:</li> <li>- Przeprowadzenie kompleksowego audytu aktualnej infrastruktury, w tym analizy sprzętu, oprogramowania, sieci oraz polityki bezpieczeństwa.</li> <li>- Identyfikacja Wymagań:</li> <li>- Konsultacje z kluczowymi interesariuszami w celu określenia wymagań technicznych i operacyjnych.</li> <li>- Zdefiniowanie wymagań funkcjonalnych i нефункциональных dotyczących systemu serwerowego.</li> </ul>
2.	Cel	<p>Wdrożenie w siedzibie Zamawiającego oferowanego rozwiązania, instalacja fizyczna w szafach teleinformatycznych, podłączenie do obecnej infrastruktury, konfiguracja urządzeń, zgodna z zaleceniami Zamawiającego wraz z pełną konfiguracją przestrzeni dyskowej i systemu operacyjnego, a także przeprowadzenie szkolenia z zakresu obsługi serwerów.</p> <p>Wdrożenie serwera musi zostać przeprowadzone przez inżyniera posiadającego fachową wiedzę zdobytą na autoryzowanych szkoleniach przeprowadzanych przez producenta oferowanego rozwiązania. Wykonawca, przedłoży certyfikat, potwierdzający, ukończenie szkolenia instalacji i wdrożeń serwerów oferowanego producenta.</p> <p>Szkolenie przeprowadzone powinno być, przez inżyniera posiadającego fachową wiedzę zdobytą na autoryzowanych szkoleniach przeprowadzanych przez producenta oferowanego rozwiązania systemu serwerowego. Wykonawca, przedłoży certyfikat, potwierdzający, ukończenie szkolenia</p> <p><b>Czas trwania szkolenia powinien potrwać nie mniej niż 10 godzin.</b></p>
3.	Projekt Architektury Systemu	Opracowanie szczegółowego projektu architektury systemu Windows Server 2022, uwzględniającego strukturę sieci, role serwera, mechanizmy zabezpieczeń i zarządzania.
4.	Wdrożenie Systemu	<p>Przedmiotem zamówienia jest wdrożenie dwóch zaawansowanych przełączników sieciowych w infrastrukturze Zamawiającego, z kluczowym celem utworzenia stosu (stack) w celu zwiększenia wydajności i niezawodności sieci. Przełączniki mają zostać połączone w stos za pomocą dedykowanych kabli o długości 1 metra, co umożliwi scentralizowane zarządzanie oraz poprawi skalowalność sieci.</p> <p>2. Zakres prac:</p> <p>2.1. Dostawa i instalacja sprzętu:</p> <p>Dostawa przełączników do lokalizacji wskazanej przez Zamawiającego.</p> <p>Instalacja fizyczna: Montaż przełączników w istniejących szafach rackowych, uwzględniająca montaż urządzeń, podłączenie do systemu zasilania awaryjnego (UPS) oraz połączenie z istniejącą infrastrukturą sieciową.</p>



	<p><b>2.2. Konfiguracja stosu (stacku):</b>  Agregacja przełączników w stos: Połączenie obu przełączników za pomocą dedykowanego kabla o długości 1 metra, tworząc pojedynczy, logiczny przełącznik z centralnym punktem zarządzania.  Konfiguracja master/slave: Ustalenie hierarchii przełączników w stosie, z przypisaniem roli urządzenia nadrzędnego (master) oraz podrzędnego (slave).  Synchronizacja konfiguracji: Zastosowanie konfiguracji globalnej, aby ustawienia dotyczące VLAN-ów, routingu oraz polityk bezpieczeństwa były identyczne na wszystkich urządzeniach w stosie.</p> <p><b>2.3. Konfiguracja sieciowa:</b>  Konfiguracja VLAN-ów: Stworzenie i konfiguracja VLAN-ów zgodnie z wymaganiami Zamawiającego, w tym VLAN-ów dedykowanych dla różnych segmentów sieci (np. administracji, serwerów, gości).  Routing między VLAN-ami: Umożliwienie routingu między VLAN-ami w celu zapewnienia bezpiecznej i wydajnej komunikacji między różnymi segmentami sieci.  Implementacja redundancji: Wdrożenie mechanizmów redundancji sieciowej poprzez konfigurację protokołów, które zapewniają nieprzerwane działanie sieci w przypadku awarii jednego z przełączników.</p> <p><b>2.4. Testowanie i weryfikacja:</b>  Testy funkcjonalne: Przeprowadzenie testów mających na celu weryfikację poprawności działania skonfigurowanego stosu, w tym synchronizacji przełączników oraz poprawności funkcjonowania sieci po ich połączeniu.  Testy wydajnościowe: Przeprowadzenie testów przepustowości oraz szybkości przełączania, aby zapewnić optymalne działanie sieci w warunkach produkcyjnych.  Testy awaryjne: Sprawdzenie skuteczności redundancji poprzez symulację awarii jednego z przełączników i weryfikację czy sieć nadal funkcjonuje bez przerw.  Zamawiający zastrzega sobie prawo do monitorowania postępu realizacji zamówienia oraz do wprowadzania zmian wynikających z potrzeb technicznych lub organizacyjnych.</p>
5.	<p><b>1. Przedmiot zamówienia</b>  Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja systemu obejmującego bibliotekę taśmową. System ma zostać zainstalowany w infrastrukturze serwerowej Zamawiającego, spełniając określone wymagania techniczne i funkcjonalne.</p> <p><b>2. Zakres zamówienia</b>  Zakres zamówienia obejmuje:</p> <p><b>Dostawa sprzętu:</b>  Dostarczenie biblioteki taśmowej zgodnej z wymaganiami technicznymi opisanymi w niniejszym OPZ.</p> <p><b>Instalacja fizyczna:</b></p> <ul style="list-style-type: none"> <li>Montaż biblioteki taśmowej w szafie rackowej 19-calowej, zgodnie z dostarczonymi szynami montażowymi.</li> <li>Podłączenie do zasilania awaryjnego (UPS) oraz do infrastruktury sieciowej Zamawiającego za pomocą odpowiednich interfejsów (np. SAS, Fibre Channel).</li> </ul> <p><b>Konfiguracja oprogramowania:</b></p> <ul style="list-style-type: none"> <li>Instalacja i konfiguracja oprogramowania do zarządzania biblioteką taśmową na serwerze lub stacji roboczej Zamawiającego.</li> <li>Ustawienie slotów, napędów oraz partycji w bibliotece taśmowej zgodnie z wymaganiami użytkownika.</li> <li>Przeprowadzenie testów funkcjonalnych oraz kalibracji.</li> </ul> <p><b>Szkolenie:</b></p>

		<ul style="list-style-type: none"> <li>Przeprowadzenie szkolenia dla zespołu IT Zamawiającego, obejmującego zarządzanie urządzeniem, podstawy obsługi, procedury konserwacji oraz procedury awaryjne.</li> </ul>
6.	Szkolenie	<p>Zakres Szkolenia: Microsoft Windows Server 2025</p> <p>1. Wprowadzenie do Windows Server 2022 Przegląd nowości i kluczowych funkcji Windows Server 2022. Wymagania systemowe i instalacyjne. Edycje Windows Server 2022 i ich zastosowania.</p> <p>2. Instalacja i Konfiguracja Przygotowanie środowiska do instalacji. Proces instalacji krok po kroku. Podstawowa konfiguracja po instalacji.</p> <p>3. Zarządzanie Tożsamościami i Dostępem Active Directory Domain Services (AD DS): Instalacja i konfiguracja. Zarządzanie użytkownikami, grupami i jednostkami organizacyjnymi. Polityki grup (Group Policy): Tworzenie, wdrażanie i zarządzanie.</p> <p>4. Zarządzanie Zasobami Sieciowymi Konfiguracja ról serwera: DNS, DHCP, File and Storage Services. Zarządzanie udostępnianiem plików i drukarek. Konfiguracja i zarządzanie systemem plików oraz przestrzenią dyskową.</p> <p>5. Wirtualizacja z Hyper-V Wprowadzenie do Hyper-V. Instalacja i konfiguracja Hyper-V. Zarządzanie maszynami wirtualnymi, sieciami wirtualnymi i przechowywaniem.</p> <p>6. Bezpieczeństwo i Ochrona Danych Zabezpieczenia w Windows Server 2022: BitLocker, Windows Defender, Firewall. Zarządzanie aktualizacjami i poprawkami (Windows Update). Kopie zapasowe i odzyskiwanie danych.</p> <p>7. Monitorowanie i Optymalizacja Systemu Narzędzia monitorowania systemu: Performance Monitor, Event Viewer. Optymalizacja wydajności serwera. Zarządzanie zasobami i wydajnością.</p> <p>8. Automatyzacja i Zarządzanie Konfiguracją Wprowadzenie do PowerShell i jego zastosowania. Automatyzacja zadań administracyjnych za pomocą skryptów PowerShell. Wprowadzenie do Windows Admin Center.</p> <p>9. Scenariusze Zaawansowane Wdrażanie i zarządzanie serwerami w chmurze (Azure). Integracja Windows Server 2022 z usługami chmurowymi. Zaawansowane scenariusze backupu i odzyskiwania.</p>

## B WDROŻENIE I SZKOLENIE DOTYCZĄCE OFEROWANYCH SERWERÓW NAS

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	<b>Charakterystyka Wdrożenia</b>	Wdrożenie w siedzibie Zamawiającego oferowanego rozwiązania, instalacja fizyczna w szafach teleinformatycznych serwerów, połączenie do obecnej infrastruktury, konfiguracja urządzeń, zgodna z Zaleceniami Zamawiającego wraz z pełną konfiguracją przestrzeni dyskowej i systemu operacyjnego, a także przeprowadzenie szkolenia z zakresu obsługi serwerów NAS złożonego z 11 modułów. Wdrożenie i Szkolenia muszą zostać <b>przeprowadzone przez certyfikowanego inżyniera</b> posiadającego fachową wiedzę zdobytą na autoryzowanych szkoleniach przeprowadzanych przez producenta oferowanego rozwiązania. <b>Dokument Wykonawca załączy do oferty.</b> <b>Czas trwania szkolenia powinien potrwać nie mniej niż 30 godzin.</b>
2.	<b>Wdrożenie systemu wersjonowania plików i konfiguracja odseparowanego środowiska testowego</b>	<p><b>1. Wersjonowanie plików</b></p> <p><b>1.1. Cel i funkcjonalność</b></p> <p>Wersjonowanie plików to funkcjonalność, która pozwala na automatyczne tworzenie wielu wersji tego samego pliku. Jest to kluczowe w przypadku współdzielenia dokumentów, pracy zespołowej oraz zabezpieczenia się przed przypadkowym nadpisaniem danych. Wersje plików są tworzone za każdym razem, gdy dokument zostaje zapisany, co umożliwia szybkie przywracanie wcześniejszych wersji w przypadku błędów.</p> <p><b>1.2. Proces wdrożenia</b></p> <p>W ramach wdrożenia na serwerze NAS, system wersjonowania plików zostanie skonfigurowany poprzez aplikację do zarządzania plikami i danymi, która pozwoli na:</p> <ul style="list-style-type: none"> <li>• Ustawienie liczby wersji plików, które mają być przechowywane,</li> <li>• Określenie okresu przechowywania starszych wersji,</li> </ul> <p>System ten umożliwi bezpieczne odzyskiwanie danych w dowolnym momencie oraz przeglądanie pełnej historii zmian plików.</p> <p><b>2. Odseparowane środowisko do testów kopii</b></p> <p><b>2.1. Cel środowiska testowego</b></p> <p>Odseparowane środowisko testowe ma na celu bezpieczne przeprowadzanie testów na zarchiwizowanych danych bez ryzyka wpływu na bieżącą operacyjną infrastrukturę. Środowisko to pozwala na testowanie aktualizacji, nowych wersji oprogramowania, a także sprawdzanie integralności kopii zapasowych.</p> <p><b>2.2. Konfiguracja środowiska</b></p> <p>Aby zapewnić pełną izolację, odseparowane środowisko testowe zostanie skonfigurowane na dedykowanym zasobie serwera NAS. Kluczowe elementy konfiguracji obejmują:</p> <ul style="list-style-type: none"> <li>• <b>Środowisko wirtualne</b>, który umożliwi tworzenie wirtualnych maszyn do przeprowadzania testów,</li> <li>• Wykorzystanie technologii klonowania kopii zapasowych, co pozwoli na szybkie przywracanie zarchiwizowanych danych w izolowanym środowisku,</li> <li>• Dostosowanie zasobów serwera, takich jak CPU, RAM i dyski, w celu spełnienia wymagań testowych bez wpływu na inne operacje serwera.</li> </ul> <p>Dzięki temu możliwe będzie testowanie różnych scenariuszy, od symulacji awarii po implementację nowych wersji aplikacji, co pozwoli na weryfikację poprawek przed ich wdrożeniem do środowiska produkcyjnego.</p> <p><b>3. Podsumowanie</b></p> <p>Wdrożenie wersjonowania plików oraz odseparowanego środowiska testowego zapewnia zaawansowaną ochronę i kontrolę nad danymi. System umożliwia bezpieczne przechowywanie wersji plików, a także elastyczne testowanie zarchiwizowanych danych bez ryzyka zakłócenia bieżącej działalności.</p>
3.	<b>Wdrożenie systemu chmurowego oraz</b>	<p><b>Opis wdrożenia systemu chmurowego do przechowywania danych</b></p> <p>1. Zakres wdrożenia:</p>

	<b>zarządzania tożsamościami</b>	<ul style="list-style-type: none"> <li>System chmurowy do przechowywania danych zostanie wdrożony w celu umożliwienia tworzenia kopii zapasowych oraz przechowywania danych użytkowników w bezpieczny sposób, zapewniając jednocześnie łatwy dostęp do danych z każdego miejsca.</li> <li>Przechowywanie danych w chmurze obejmuje co najmniej 5 TB dostępnej przestrzeni, która będzie wykorzystana do archiwizacji dokumentów, plików multimedialnych oraz danych aplikacyjnych.</li> </ul> <p><b>2. Funkcje systemu:</b></p> <ul style="list-style-type: none"> <li>System wspiera automatyczne wersjonowanie plików, co pozwala na przywracanie wcześniejszych wersji dokumentów.</li> <li>Usługa umożliwia przechowywanie danych w środowisku hybrydowym, gdzie dane są przechowywane zarówno w lokalnej infrastrukturze zamawiającego, jak i w chmurze, zapewniając elastyczność oraz zwiększoną niezawodność.</li> <li>System oferuje zaawansowane funkcje szyfrowania danych w trakcie ich przesyłania oraz przechowywania, co gwarantuje zgodność z wymaganiami bezpieczeństwa i przepisami RODO.</li> </ul> <p><b>3. Integracja z istniejącą infrastrukturą:</b></p> <ul style="list-style-type: none"> <li>System będzie zintegrowany z lokalnymi serwerami zamawiającego, co pozwoli na sprawne przesyłanie danych do chmury. Wdrożenie obejmie synchronizację danych w czasie rzeczywistym, co umożliwi zamawiającemu natychmiastowy dostęp do aktualnych kopii zapasowych.</li> </ul> <p><b>1. Opis wdrożenia systemu zarządzania tożsamościami</b></p> <p><b>2. Zakres wdrożenia:</b></p> <ul style="list-style-type: none"> <li>System zarządzania tożsamościami użytkowników zostanie wdrożony w celu scentralizowanego zarządzania dostępem do zasobów cyfrowych organizacji. System ten umożliwi bezpieczną autoryzację i uwierzytelnianie użytkowników za pomocą mechanizmu jednokrotnego logowania (SSO).</li> </ul> <p><b>3. Funkcje systemu:</b></p> <ul style="list-style-type: none"> <li>Umożliwia synchronizację z lokalnymi serwerami katalogowymi zamawiającego, takimi jak Active Directory, co pozwala na centralne zarządzanie kontami użytkowników i grupami.</li> <li>System wspiera uwierzytelnianie dwuskładnikowe (2FA), co dodatkowo zabezpiecza dostęp do zasobów i zwiększa poziom ochrony przed nieautoryzowanym dostępem.</li> </ul> <p><b>4. Zarządzanie dostępami i integracja:</b></p> <ul style="list-style-type: none"> <li>Wdrożenie obejmuje pełną integrację z istniejącą infrastrukturą sieciową, umożliwiając łatwe przypisywanie uprawnień użytkownikom do określonych zasobów, aplikacji oraz usług.</li> <li>System zapewnia automatyzację procesów resetowania haseł oraz ich zarządzania przez dedykowanego menedżera haseł, co ułatwi użytkownikom bezpieczne przechowywanie oraz aktualizację haseł.</li> </ul> <p><b>5. Szkolenie i wsparcie:</b></p> <ul style="list-style-type: none"> <li>W ramach wdrożenia, dostawca systemu zobowiązuje się do przeprowadzenia szkoleń dla pracowników zamawiającego, obejmujących obsługę systemu zarządzania tożsamościami oraz systemu przechowywania danych.</li> </ul>
4.	<b>Szkolenie</b>	<p><b>1. Zarządzanie przechowywaniem.</b></p> <ol style="list-style-type: none"> <li>Omówienie dostępnych typów RAID, ich specyfikacji, algorytmu działania, a także dobór najlepszego wariantu adekwatnie do przedstawionych wymagań. Szczegółowe omówienie tradycyjnych typów RAID takich jak RAID 1, 5, 6, 10 oraz niestandardowych SHR, SHR-2 i F1.</li> <li>Omówienie dostępnych systemów plików, ich specyfikacji, funkcjonalności oraz architektury, a także dobór najlepszego wariantu do przedstawionych wymagań.</li> <li>Omówienie specyfikacji dysków HDD i SSD kompatybilnych z posiadanym serwerem NAS pod kątem zastosowania w długoterminowym przechowywaniu danych. Objasnienie różnic w mechanizmie zapisu na dyskach talerzowych oraz flash'owych.</li> <li>Wpływ kluczowych parametrów SMART na działanie dysków w macierzy.</li> <li>Procedura wymiany uszkodzonego dysku w grupie RAID. Rozbicie tematu na różne przypadki wraz z symulacją awarii. Wady i zalety stosowania dysków zapasowych.</li> </ol>

- f) Dostępne opcje rozbudowy istniejącej puli pamięci oraz ograniczenia z nimi związane z podziałem na zastosowane typy RAID.
- g) Możliwości skalowalności urządzenia pod kątem zastosowania większej ilości dysków, a co za tym idzie zwiększenia pojemności istniejącej puli pamięci lub utworzenia nowej.
- h) Wybór odpowiedniego priorytetu synchronizacji grupy RAID zależnie od zastosowanych dysków i przeznaczenia serwera NAS. Analiza obciążenia systemu i wykorzystania dysków przy jednoczesnym wykorzystywaniu zasobów serwera przez stacje klienckie.
- i) Omówienie rodzajów testów SMART, ich cech charakterystycznych, przeznaczenia oraz przypadków zastosowania. Implementacja sensownego i bezpiecznego harmonogramu wykonywania testów, pełna automatyzacja poprzez dedykowane skrypty.
- j) Dostępne mechanizmy wpływające na zwiększenie szybkości odczytu i zapisu danych, wymagania związane z implementacją takiego rozwiązania, wady i zalety zależnie od rodzaju środowiska serwerowego i wykorzystywanych aplikacji. Analiza żywotności wybranych nośników, symulacja czasu pracy oraz retencji w celu utrzymania najwyższego poziomu wydajności pamięci podręcznej w danej jednostce czasu z uwzględnieniem szacunkowych ilości zapisu i odczytu danych.
- k) Algorytm szyfrowania danych – praktyczne zastosowanie, wpływ na obciążenie serwera i wydajność systemu, możliwości wykorzystania szyfrowania na różnego typu zasobach. Ograniczenia związane z włączeniem szyfrowania, zagrożenia wynikające z niezastosowania takiego algorytmu.
- l) Kopiowanie przy zapisie (ang. copy on write) – zasada działania na przykładzie systemu plików btrfs. Zastosowanie praktyczne, wady i zalety, ograniczenia i wymagania.

## 2. Użytkownicy i grupy.

- a) Zarządzanie użytkownikami i grupami lokalnymi, konfiguracja strategii bezpiecznego logowania, automatyzacja procesu tworzenia nowych użytkowników i wdrażania ich do korzystania z systemu.
- b) Zarządzanie użytkownikami i grupami domenowymi, podłączanie serwera NAS jako klienta domeny, a także tworzenie niezależnego kontrolera domeny opartego o natywne rozwiązanie dostępne w systemie operacyjnym serwera NAS. Pełne wdrożenie testowe z uwzględnieniem zarządzania kontrolerem domeny w sposób rozszerzony poprzez dodatek RSAT, konfigurację profili mobilnych dla użytkowników domenowych z wykorzystaniem zasobów magazynowych serwera NAS. Konfiguracja polis związanych z automatyczną instalacją wskazanych programów na systemach klienckich.
- c) Omówienie zasad nadawania uprawnień użytkownikom i grupom z wyszczególnieniem podziału na uprawnienia Unix i ACL. Implementacja obu wariantów w celu wyboru najbardziej odpowiedniego do postawionych wymagań.

## 3. Foldery współdzielone.

- a) Zasada funkcjonowania folderów współdzielonych w systemie operacyjnym. Powiązanie z systemem plików działającym na podstawie wolumenów.
- b) Omówienie działania systemu plików btrfs pod kątem utrzymania integralności danych z wykorzystaniem dodatkowych sum kontrolnych.
- c) Wskazanie i wyjaśnienie algorytmu wykorzystywanego do kompresji danych. Wykorzystanie praktyczne wraz z testami oszczędności zajmowanej przez pliki przestrzeni po włączeniu kompresji.
- d) Szczegółowe wytłumaczenie funkcjonalności WORM (ang. Write Once Read Many) działającej na poziomie folderów współdzielonych. Przykłady wykorzystania praktycznego oraz korzyści z tego płynące.



- e) Foldery domowe – zasada funkcjonowania dla użytkowników lokalnych i domenowych.
- f) Metody udostępniania plików osobom z zewnątrz z zachowaniem zasad bezpieczeństwa tj. szyfrowania transferu oraz zabezpieczenia dostępu przed osobami nieuprawnionymi.

#### 4. Ustawienia sieciowe.

- a) Zasada działania więcej niż dwóch interfejsów LAN w serwerze. Wyjaśnienie domyślnej adresacji LAN oraz przykładowa konfiguracja w sieci LAN bez serwera DHCP.
- b) Agregacja łączy ze szczegółowym omówieniem specyfikacji każdego dostępnego trybu dedykowanego dla przełączników bez interfejsu zarządzania oraz dla tych z interfejsem zarządzania i wsparciem dla protokołu LACP (ang. Link Aggregation Control Protocol), standard 802.3ad.
- c) Statyczny routing po stronie serwera NAS, ustawienia zasad filtrowania ruchu i sterowania ruchem z podziałem na konkretne usługi i porty.
- d) Konfiguracja podstawowych parametrów połączeniowych serwera NAS z siecią Internet. Wyjaśnienie zasady działania takiego połączenia w momencie korzystania z kilku interfejsów LAN. Wady i zalety zamiennego stosowania nazwy serwera do połączeń CIFS/SMB zamiast adresu IP.
- e) Zasada działania serwera proxy i przykład wykorzystania w realnym środowisku.
- f) Konfiguracja niestandardowych portów zarządzania. Wyszczególnienie dostępnych metod lokalnego i zdalnego zarządzania serwerem poprzez interfejs Web UI oraz linię komend.

#### 5. Kopie zapasowe i ochrona danych.

- a) Zasady bezpiecznego przechowywania danych z przykładem implementacji w omawianym środowisku.
- b) Metody wykonywania kopii zapasowej z uwzględnieniem różnego typu nośników tj. dysków USB, obudów RAID, bibliotek LTO, innych serwerów fizycznych oraz serwerów NAS.
- c) Szczegółowe omówienie metod replikacji danych na inny serwer NAS tego samego producenta oraz porównanie procesu do replikacji na inne rozwiązanie firmy trzeciej. Wskazanie najlepszej dostępnej metody do wykorzystania w sieci LAN oraz poprzez WAN.
- d) Wyjaśnienie zasady działania mechanizmu migawek z wykorzystaniem kopiowania przy zapisie. Przedstawienie możliwości implementacji harmonogramu wykonywania migawek w systemie oraz związanych z tym najlepszych praktyk. Analiza potencjalnego wykorzystania przestrzeni przez migawki w długoterminowym procesie ich przechowywania oraz omówienie dostępnych strategii retencji wersji.
- e) Metody odzyskiwania danych z migawek z opcją przywracania lokalnego oraz zdalnego. Wyjaśnienie różnic i cech szczególnych obu metod.
- f) Utworzenie i przedstawienie w praktyce zasady działania replikacji migawek z uwzględnieniem przełączania awaryjnego między serwerami. Szczególnie w przypadku podłączenia do kontrolera domeny i odtwarzania danych wraz z uprawnieniami na serwerze docelowym.
- g) Przedstawienie sposobów wykonywania kopii zapasowych do środowisk chmurowych.

#### 6. Kłaster wysokiej dostępności.

- a) Omówienie wymagań dotyczących utworzenia klastra wysokiej dostępności z dwóch takich samych serwerów NAS.
- b) Omówienie wymagań i ograniczeń dotyczących utworzenia klastra wysokiej dostępności z dwóch różnych serwerów NAS.
- c) Zasada działania klastra SHA (ang. Synology High Availability). Wady i zalety oraz korzyści płynące z zastosowania rozwiązania klastrowego jako główne miejsce składowania danych i różnego typu usług.

d) Algorytm przełączania awaryjnego serwerów w klastrze. Jakie wymagania musi spełniać połączenie między serwerami, jakie ograniczenia występują, jakie problemy mogą wystąpić oraz jak w praktyce odczuwalna będzie praca na zasobach klastra SHA.

#### **7. Kopie zapasowe komputerów, serwerów i maszyn wirtualnych.**

- a) Omówienie dostępnych metod wykonywania kopii zapasowych komputerów PC z zaprezentowaniem działania w praktyce z podziałem na kopie plikowe oraz bare-metal.
- b) Opracowanie systemu wdrażania odpowiedniego rozwiązania do kopii zapasowej na dużą skalę.
- c) Metody przywracania danych dostępne dla zwykłych użytkowników oraz administratorów. Praktyczne zastosowanie oraz instruktarz dotyczący każdej z dostępnych metod na przykładzie komputera z systemem Windows oraz Linux.
- d) Możliwości masowego konfigurowania zasad tworzenia kopii zapasowych.
- e) Wyjaśnienie i zaprezentowanie realnego wpływu szyfrowania i kompresji transferu danych na komputery lokalne.
- f) Strategie przechowywania danych kopii zapasowych w planie długoterminowym z możliwością przywrócenia kopii zapasowej sprzed 6, 12, i 18 miesięcy.
- g) Kontrola integralności danych kopii zapasowych i testowe odtwarzanie.
- h) Możliwości automatyzacji procesu odtwarzania danych w przypadku awarii komputera.
- i) Testowe przywracanie obrazu kopii w formie maszyny wirtualnej w natywnym wirtualizatorze dostępnym na serwerze NAS oraz na zewnętrznych wirtualizatorach.
- j) Omówienie różnic w działaniu środowisk wirtualizacji opartych o KVM oraz QEMU.
- k) Wyjaśnienie mechanizmów wpływających na redukcję zajmowanej przez kopie zapasowe przestrzeni takich jak deduplikacja i kompresja. Wykazanie algorytmu działania oraz wpływu na żywotność dysków.
- l) Przedstawienie metody replikacji centralnego repozytorium kopii zapasowych na zapasowy serwer NAS z opcją przełączenia klientów na tę jednostkę i wznowienia harmonogramów kopii zapasowych.
- m) Metody wykonywania kopii zapasowych systemów bazodanowych działających na serwerach fizycznych z systemami operacyjnymi z rodziny Windows oraz Linux oraz adekwatne metody przywracania.
- n) Wykonywanie kopii zapasowych maszyn wirtualnych z różnych środowisk wirtualizacji obsługiwanych przez zintegrowane narzędzie dostępne w systemie serwera NAS. Wyjaśnienie zasady działania mechanizmu kopii, opcji przywracania natychmiastowego oraz pełnego.

#### **8. Serwer poczty.**

- a) Omówienie dostępnych pakietów pozwalających na uruchomienie serwera pocztowego. Jakie są kluczowe różnice, plan licencjonowania, wady i zalety.
- b) Wytypowanie odpowiedniego pakietu pozwalającego na utworzenie serwera pocztowego i na jego przykładzie zaprezentowanie praktycznego działania.
- c) Wymagania dotyczące utworzenia serwera.
- d) Wyjaśnienie zarządzania domeną oraz rekordami DNS.
- e) Przekierowywanie portów wymaganych do działania usług na serwerze NAS. Niebezpieczeństwo płynące z tego typu praktyk.
- f) Pełnoprawne uruchomienie serwera pocztowego po przeprowadzonej konfiguracji. Testy działania usług SMTP, IMAP i POP3.
- g) Obsługa kont pocztowych za pomocą natywnego klienta oraz oprogramowania firm trzecich.
- h) Monitorowanie stanu serwera pocztowego, potencjalnych zagrożeń, filtrowanie poczty oraz włączanie silników antyspamowych.

- i) Praktyczne zaprezentowanie procedury migracji danych z istniejącego serwera pocztowego na nowe rozwiązanie zaimplementowane na serwerze NAS.

#### 9. System monitoringu.

- Omówienie wymagań związanych z wdrożeniem systemu monitoringu opartego o serwer NAS z centralnym zarządzaniem podległymi serwerami nagrywającymi.
- Prezentacja funkcjonalności i zarządzania takim systemem w praktyce z wykorzystaniem co najmniej dwóch różnego typu kamer IP. Minimum jedna standardowa i jedna sterowana (ang. PTZ).
- Konfiguracja przestrzeni przechowywania nagrań. Najlepsza dopuszczalna strategia retencji.
- Analiza wydajności zapisu z wykorzystaniem systemów plików ext4 i btrfs. Wybór odpowiedniego rozwiązania pod kątem najlepszych osiągnięć.
- Dodawanie różnego typu kamer do systemu monitoringu – kompatybilnych oraz z wykorzystaniem protokołu ogólnego ONVIF.
- Przetestowanie działania wykrywania ruchu i innych podobnych funkcjonalności na poziomie zarządzania kamery oraz systemu monitoringu.
- Automatyzacja dotycząca powiadamiania o zaistniałych zdarzeniach wykrytych przez system monitoringu.
- Sposoby na redukcję przestrzeni zajmowanej przez nagrania, archiwizacja oraz tworzenie tzw. timelapse'ów.

#### 10. Zarządzanie systemem.

- Zarządzanie serwerem NAS i systemem operacyjnym pracującym na nim poprzez centralny system zarządzania, a także aplikacje mobilne. Wyszczególnienie ograniczeń i wymagań dotyczących każdej metody.
- Zabezpieczenie serwera poprzez wdrożenie zasady automatycznego blokowania adresów IP, białej oraz czarnej listy, filtrowania ruchu przychodzącego.
- Wdrożenie uwierzytelniania dwuskładnikowego dla użytkowników posiadających zdalny dostęp do zarządzania serwerem.
- Konfiguracja systemu powiadomień wykorzystującego dedykowany serwer SMTP lub pośredniczące konto e-mail.
- Prezentowanie dostępnych narzędzi monitorowania stanu różnego typu urządzeń, które udostępniają stan poszczególnych parametrów i ustawień poprzez protokół SNMP.
- Omówienie zasad oraz metod wykonywania aktualizacji oprogramowania serwera NAS w przypadku pojedynczego serwera oraz klastra wysokiej dostępności.
- Automatyzacja procesu wykonywania kopii zapasowej podstawowej konfiguracji systemu. Objasnienie co dokładnie zawiera ta kopia, w jaki sposób można ją przywrócić i jakie są ograniczenia z tym związane.

#### 11. Sprzęt i konserwacja.

- Szczegółowe omówienie specyfikacji sprzętowej oferowanego serwera NAS oraz możliwości jego rozbudowy.
- Prezentowanie instrukcji wymiany pamięci RAM oraz montowania dodatkowych kart rozszerzeń.
- Omówienie procesu wymiany podzespołów podczas pracy takich jak dyski HDD.
- Prezentowanie schematu działania w przypadku wystąpienia problemów z połączeniem do systemu zarządzania serwerem NAS lub w przypadku zatrzymania działania niektórych usług.
- Symulacja różnych typów awarii, które mogą wystąpić podczas użytkowania serwera i sposobów szybkiego rozwiązywania powstałych problemów.

- f) Instruktarz dotyczący bezpiecznego czyszczenia serwera NAS z wymontowaniem niektórych podzespołów.

## C WDROŻENIE I SZKOLENIE OFEROWANYCH PRZEŁĄCZNIKÓW

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	Wdrożenie	<p><b>Etapy wdrożenia</b></p> <p><b>3.1 Planowanie infrastruktury</b></p> <p>Przełączniki zostaną rozmieszczone w warstwie dostępowej oraz dystrybucyjnej sieci. Porty uplink 10G umożliwią szybką komunikację z przełącznikami rdzeniowymi i serwerami, zapewniając płynny przepływ danych.</p> <p><b>3.2 Montaż i konfiguracja</b></p> <ul style="list-style-type: none"> <li>• <b>Fizyczne rozmieszczenie przełączników:</b> montaż przełączników w szafach RACK w lokalizacjach zgodnych z planem sieciowym.</li> <li>• <b>Podłączenie kabli zasilających i sieciowych:</b> porty PoE+ pozwolą na jednoczesne dostarczenie danych i zasilania do urządzeń końcowych (np. punktów dostępowych, kamer).</li> <li>• <b>Konfiguracja warstwy L3:</b> konfiguracja trasowania dynamicznego z użyciem protokołów OSPF lub RIP, co zapewni optymalizację tras i wydajność sieci. Każdy przełącznik będzie zarządzany centralnie, a VLAN-y zostaną skonfigurowane w celu separacji ruchu wewnątrz organizacji.</li> </ul> <p><b>3.3 Testowanie</b></p> <p>Po zakończeniu konfiguracji nastąpi etap testowania, obejmujący:</p> <ul style="list-style-type: none"> <li>• sprawdzenie poprawności zasilania urządzeń końcowych przez PoE+,</li> <li>• testowanie przepustowości portów uplink 10G,</li> <li>• weryfikację poprawności funkcjonowania VLAN-ów oraz trasowania dynamicznego.</li> </ul> <p><b>4. Monitorowanie i zarządzanie</b></p> <p>Po zakończeniu wdrożenia przełączniki zostaną włączone do systemu monitorowania sieciowego. Obsługiwane protokoły (SNMP, interfejs webowy) pozwolą na stałe monitorowanie wydajności oraz zdalne zarządzanie urządzeniami. Regularne aktualizacje oprogramowania oraz polityki bezpieczeństwa będą wdrażane zgodnie z harmonogramem konserwacji.</p>

## D WDROŻENIE I SZKOLENIE SYSTEMU NAC DO IZOLACJI SIECI LAN W SIEDZIBIE ZAMAWIAJĄCEGO

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	Wdrożenie i szkolenie	<p><b>Etap I. Przygotowanie wdrożenia</b></p> <p>1. Uzgodnienie wymagań technicznych i przygotowanie przez Klienta zasobów niezbędnych do realizacji prac wdrożeniowych</p> <p><b>Etap II: Wdrożenie rozwiązania</b></p> <ol style="list-style-type: none"> <li>1. Import maszyny wirtualnej na platformę wirtualizacyjną (VMware lub Hyper-V)</li> <li>2. Konfiguracja parametrów sieciowych i lokalnych interfejsów sieciowych</li> <li>3. Konfiguracja powiadomień mailowych</li> <li>4. Konfiguracja integracji z Active Directory</li> <li>5. Konfiguracja integracji z Windows Management Instrumentation (WMI)</li> <li>6. Krótki instruktaż dla administratora</li> <li>7. Podsumowanie wdrożenia - ewentualne pytania</li> <li>8. Odbiór prac wdrożeniowych</li> </ol> <p><b>Etap III. Szkolenie: konfiguracja i administrowanie rozwiązaniem NAC (4 godz. zdalnie)</b></p> <p>Agenda:</p> <ol style="list-style-type: none"> <li>1. NAC - sposób działania i wykorzystanie w infrastrukturze IT</li> </ol>

2. Interfejs administratora
3. Konfiguracja sieciowa rozwiązania
4. Monitorowanie sieci i blokowanie dostępu (Device Manager, Network Map)
5. Ochrona przed spoofingiem (fingerprinting)
6. Powiadomienia mailowe
7. Automatyczna klasyfikacja urządzeń (Device Profiler, Auto Trust)
8. Zarządzanie dostępem (Roles & Access, ACLs)
9. Integracja z innymi systemami (AD, AV, WMI, Syslog & Email Orchestration)
10. Rejestrowanie urządzeń prywatnych i dostęp gości (Captive Portal)
11. Raporty (Device Manager Reports, Network Inventory)
12. Aktualizacja firmware

Etap IV. Konsultacje powdrożeniowe (4 godz. zdalnie)

1. Przegląd działania rozwiązania 1-3 miesiące od zakończenia wdrożenia

2. Odpowiedzi na pytania związane z eksploatacją rozwiązania NAC

Wymaga się, aby dostawca przedstawił:

- oświadczenie producenta o posiadaniu przez dostawcę kwalifikacji technicznych, niezbędnych do wykonania wdrożenia oferowanego rozwiązania i szkolenia należy załączyć do oferty

- osobowy certyfikat inżynierski pracownika, która będzie wykonywał wdrożenie , należy załączyć do oferty

## E WDROŻENIE I SZKOLENIE SYSTEMU ZAPOBIEGANIA WYCIEKOM DANYCH I INFORMACJI (DLP)

L.P	Parametr	Charakterystyka (wymagania minimalne)
1	Wdrożenie i konfiguracja	<p>1. Przedmiot zamówienia Przedmiotem zamówienia jest wdrożenie systemu klasy DLP (Data Loss Prevention) na infrastrukturze serwerowej Zamawiającego. Wdrożenie obejmuje konfigurację serwera bazodanowego, instalację i konfigurację oprogramowania na serwerze wirtualnym oraz przeszkolenie personelu Zamawiającego.</p> <p>2. Zakres zamówienia Zakres zamówienia obejmuje następujące elementy: Konfiguracja serwera bazodanowego: Przygotowanie serwera bazodanowego: Ustawienie środowiska bazodanowego zgodnie z wymaganiami systemu DLP. Konfiguracja instancji bazy danych obejmująca odpowiednie parametry wydajnościowe i bezpieczeństwa. Integracja z systemem DLP: Połączenie bazy danych z oprogramowaniem DLP, zapewniając jej optymalną współpracę i wydajność. Instalacja i konfiguracja na serwerze wirtualnym: Przygotowanie środowiska serwera wirtualnego: Instalacja systemu operacyjnego oraz wszystkich niezbędnych komponentów na serwerze wirtualnym dostarczonym przez Zamawiającego. Instalacja oprogramowania DLP: Zainstalowanie systemu DLP na serwerze wirtualnym, zgodnie z wymaganiami technicznymi dostawcy oprogramowania. Konfiguracja systemu: Ustawienie reguł bezpieczeństwa, polityk monitorowania i ochrony danych zgodnie z potrzebami Zamawiającego. Konfiguracja modułów monitorowania, raportowania oraz alertów w systemie DLP. Integracja z infrastrukturą sieciową: Połączenie z istniejącymi systemami: Integracja systemu DLP z infrastrukturą sieciową Zamawiającego, w tym z serwerami plików, pocztą e-mail oraz innymi krytycznymi usługami. Testowanie połączeń i funkcjonalności: Weryfikacja poprawności działania systemu DLP w rzeczywistym środowisku produkcyjnym. Testowanie reguł ochrony oraz raportowania w celu zapewnienia zgodności z założonymi wymaganiami. Szkolenie: Szkolenie zespołu IT Zamawiającego: Przeprowadzenie szkolenia dla zespołu odpowiedzialnego za zarządzanie i obsługę systemu DLP. Szkolenie obejmuje: Podstawy konfiguracji i zarządzania systemem DLP. Zarządzanie incydentami i alertami.</p>



Tworzenie i modyfikowanie polityk bezpieczeństwa.  
 Monitorowanie i raportowanie działań w systemie DLP.  
 Szkolenie minimum 6 godzin  
 Dokumentacja: Dostarczenie szczegółowej dokumentacji dotyczącej wdrożonego systemu oraz

## F WDROŻENIE I SZKOLENIE OPROGRAMOWANIA AV DEDYKOWANEG DO OCHRONY SERWERÓW

L.P	Parametr	Charakterystyka (wymagania minimalne)
1	Wdrożenie i szkolenie	<p>1. Przedmiot zamówienia          Przedmiotem zamówienia jest wdrożenie oraz konfiguracja zintegrowanego systemu zabezpieczeń obejmującego zaawansowane narzędzia do wykrywania zagrożeń, zarządzania podatnościami oraz monitorowania aktywności sieciowej. System ma zostać wdrożony na infrastrukturze Zamawiającego, z pełną konfiguracją oraz przeszkoleniem personelu.</p> <p>2. Zakres zamówienia          Zakres zamówienia obejmuje następujące elementy:</p> <ol style="list-style-type: none"> <li>Instalacja i konfiguracja narzędzia do wykrywania zagrożeń (XDR):             <ul style="list-style-type: none"> <li>Przygotowanie środowiska serwerowego: Instalacja oprogramowania na dedykowanych serwerach lub wirtualnych maszynach, zapewniająca optymalną wydajność i skalowalność systemu.</li> <li>Konfiguracja agentów: Instalacja agentów monitorujących na stacjach roboczych, serwerach oraz innych urządzeniach sieciowych w infrastrukturze Zamawiającego.</li> <li>Ustawienie reguł wykrywania: Skonfigurowanie reguł wykrywania zagrożeń, monitorowania incydentów oraz reagowania na wykryte zagrożenia zgodnie z politykami bezpieczeństwa Zamawiającego.</li> <li>Integracja z istniejącymi systemami: Połączenie systemu z narzędziami zarządzania logami (SIEM) oraz innymi elementami infrastruktury IT w celu zapewnienia kompleksowej ochrony.</li> </ul> </li> <li>Instalacja i konfiguracja narzędzia do zarządzania podatnościami:             <ul style="list-style-type: none"> <li>Skany początkowe: Przeprowadzenie początkowych skanów podatności na wszystkich krytycznych zasobach IT Zamawiającego.</li> <li>Konfiguracja harmonogramów skanowania: Ustalenie regularnych harmonogramów skanowania, które będą automatycznie identyfikować nowe podatności oraz oceniać ryzyko związane z nimi.</li> <li>Raportowanie: Konfiguracja systemu raportowania, który będzie dostarczał regularne raporty na temat stanu zabezpieczeń oraz rekomendacje dotyczące działań naprawczych.</li> <li>Integracja z narzędziem XDR: Skonfigurowanie automatycznego przekazywania wyników skanowania do systemu wykrywania zagrożeń, co umożliwi bardziej dynamiczne reagowanie na wykryte podatności.</li> </ul> </li> <li>Instalacja i konfiguracja narzędzia do monitorowania aktywności sieciowej:             <ul style="list-style-type: none"> <li>Monitorowanie w czasie rzeczywistym: Ustawienie monitoringu sieciowego w celu wykrywania nietypowych zachowań i potencjalnych zagrożeń w czasie rzeczywistym.</li> <li>Analiza ruchu sieciowego: Skonfigurowanie analizy ruchu sieciowego, z naciskiem na wykrywanie anomalii, które mogą wskazywać na próby włamań lub inne formy cyberataków.</li> <li>Zarządzanie alertami: Konfiguracja systemu alertów, który powiadomi odpowiednie osoby lub zespoły w przypadku wykrycia podejrzanych działań.</li> </ul> </li> <li>Szkolenie personelu:             <ul style="list-style-type: none"> <li>Szkolenie z obsługi systemu: Przeprowadzenie szkolenia dla zespołu IT Zamawiającego, obejmującego zarządzanie każdym z wdrożonych narzędzi, w tym:                 <ul style="list-style-type: none"> <li>Monitorowanie i zarządzanie wykrytymi zagrożeniami.</li> <li>Tworzenie i modyfikowanie polityk bezpieczeństwa.</li> <li>Przeprowadzanie skanów podatności oraz interpretacja wyników.</li> <li>Zarządzanie i reagowanie na alerty związane z aktywnością sieciową.</li> <li>Szkolenie minimum 10 godzin</li> </ul> </li> </ul> </li> <li><b>Dla zapewnienia wysokiego poziomu usług podmiot wdrażający rozwiązanie musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem.</b></li> </ol>

## G WDROŻENIE I SZKOLENIE OPROGRAMOWANIA XDR NA SERWERACH

L.P	Parametr	Charakterystyka (wymagania minimalne)
1	Wdrożenie	<p>Wdrożenie systemów ochrony opartych na zintegrowanej platformie bezpieczeństwa składa się z kilku kluczowych etapów:</p> <ol style="list-style-type: none"> <li><b>1. Analiza Wymagań</b> Proces wdrożenia rozpoczyna się od oceny aktualnej infrastruktury klienta, w tym liczby chronionych serwerów, potrzeb w zakresie zabezpieczeń danych i tożsamości, oraz możliwości integracji z istniejącymi systemami zarządzania i chmurowymi.</li> <li><b>2. Instalacja Oprogramowania</b> Po określeniu wymagań następuje instalacja oprogramowania na serwerach oraz urządzeniach końcowych. Systemy zabezpieczające chronią serwery, stacje robocze i urządzenia mobilne przed zagrożeniami, wykorzystując zaawansowane mechanizmy wykrywania zagrożeń oraz ochrony przed złośliwym oprogramowaniem.</li> <li><b>3. Ochrona Danych i Tożsamości</b> Zintegrowany system monitoruje zarówno urządzenia, jak i aktywność użytkowników w czasie rzeczywistym. Obejmuje to m.in. ochronę tożsamości, która zabezpiecza dostęp do krytycznych zasobów oraz monitoruje zagrożenia związane z nieautoryzowanym dostępem.</li> <li><b>4. Konfiguracja Ochrony Chmurowej</b> W ramach wdrożenia systemów ochrony współpracy i chmury, zabezpieczane są platformy do współpracy i przechowywania danych, w tym ochrona poczty elektronicznej, przestrzeni współdzielonych oraz przesyłanych plików.</li> <li><b>5. Zarządzanie i Optymalizacja</b> System zarządzania bezpieczeństwem pozwala na bieżąco monitorować stan ochrony, reagować na incydenty oraz optymalizować polityki bezpieczeństwa. Wykorzystanie automatycznego wykrywania zagrożeń oraz mechanizmów uczenia maszynowego zwiększa skuteczność ochrony.</li> </ol>
2	Szkolenie	<p>Szkolenie ma na celu zapoznanie użytkowników z zaawansowanymi narzędziami ochrony, które zapewniają kompleksową ochronę serwerów, systemów operacyjnych oraz danych przetwarzanych na dostarczonych serwerach oraz pozostałej infrastrukturze serwerowej Zamawiającego. Obejmuje ono praktyczne wdrożenie systemów służących do detekcji zagrożeń, ochrony punktów końcowych, zarządzania tożsamościami oraz monitorowania środowisk chmurowych. Ważnym elementem jest także integracja rozwiązań wspierających ochronę danych w środowiskach współpracy, takich jak platformy komunikacyjne i współdzielone przestrzenie danych.</p> <p><b>Wprowadzenie do systemów ochrony serwerów i punktów końcowych:</b></p> <ul style="list-style-type: none"> <li>• Omówienie architektury nowoczesnych narzędzi ochrony, zapewniających wielopoziomą ochronę serwerów oraz urządzeń końcowych.</li> <li>• Konfiguracja polityk bezpieczeństwa dla serwerów, dostosowanych do specyfiki środowiska produkcyjnego i wymagań audytowych.</li> <li>• Monitorowanie i reagowanie na incydenty z wykorzystaniem wbudowanych narzędzi do analizy zagrożeń w czasie rzeczywistym.</li> </ul>

**Zarządzanie i ochrona tożsamości użytkowników:**

- Implementacja zaawansowanych mechanizmów zarządzania tożsamościami w oparciu o scentralizowane repozytoria danych.
- Synchronizacja użytkowników i grup z systemami lokalnymi oraz automatyzacja procesów zarządzania dostępami.
- Ochrona tożsamości użytkowników przy użyciu narzędzi wykrywających anomalie oraz potencjalne ataki wykorzystujące dane logowania.

**Ochrona środowisk chmurowych:**

- Konfiguracja zabezpieczeń dla usług chmurowych, zapewniających ochronę przed zagrożeniami wewnętrznymi oraz zewnętrznymi.
- Mechanizmy tworzenia kopii zapasowych oraz przywracania danych w środowiskach chmurowych.
- Praktyczne ćwiczenia z konfiguracji polityk bezpieczeństwa, które mają na celu ochronę danych przechowywanych w chmurze.

**Ochrona współpracy i platform komunikacyjnych:**

- Konfiguracja zabezpieczeń dla środowisk współpracy, w tym narzędzi do zarządzania dokumentami, komunikacją zespołową i przechowywaniem plików.
- Zasady wdrażania polityk bezpieczeństwa dla platform pocztowych, przestrzeni współdzielonych oraz narzędzi komunikacyjnych.
- Detekcja zagrożeń oraz monitorowanie anomalii w komunikacji i współdzieleniu plików.

**Wykorzystanie sztucznej inteligencji w analizie zagrożeń:**

- Omówienie możliwości sztucznej inteligencji w analizie danych z systemów bezpieczeństwa.
- Praktyczne ćwiczenia w zakresie konfiguracji narzędzi do monitorowania i detekcji zaawansowanych zagrożeń przy pomocy uczenia maszynowego.
- Integracja systemów analitycznych z mechanizmami automatycznego reagowania na incydenty bezpieczeństwa.

**Zarządzanie zagrożeniami i tworzenie raportów:**

- Konfiguracja dashboardów do monitorowania aktywności w czasie rzeczywistym.
- Tworzenie raportów z incydentów bezpieczeństwa oraz analiza danych historycznych.
- Zautomatyzowane raportowanie zagrożeń oraz optymalizacja systemu w oparciu o wnioski z analizy.

