



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Załącznik nr 1 do SWZ. Szczegółowy opis przedmiotu zamówienia

Dotyczy zamówienia publicznego pn. Dostawa serwerów, urządzeń pamięci masowej, urządzeń sieciowych, zasilaczy awaryjnych i oprogramowania w ramach projektu „Cyberbezpieczny Samorząd”

Ogólne warunki realizacji zamówienia

1. Przedmiot zamówienia obejmuje dostawy do siedziby Zamawiającego, tj. Urzędu Gminy Dzierzkowice w zakresie i ilościach wskazanych w zestawieniu rzeczowo – ilościowym.
2. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
3. Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji (tzw. End of Life).
4. Dostarczany sprzęt i oprogramowanie muszą pochodzić z oficjalnego kanału dystrybucyjnego w UE.
5. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
6. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
7. Zamawiający dopuszcza rozwiązania równoważne. Ogólne zasady równoważności rozwiązań:
 - a. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
 - b. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
 - c. Użycie w opisie przedmiotu zamówienia nazw rozwiązań, materiałów i urządzeń służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.
 - d. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne.



- e. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
- f. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
- g. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
- h. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.
- i. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Postępowanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy.



Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

Zestawienie rzeczowo - ilościowe

Lp.	Przedmiot dostawy	Ilość
1.	Firewall sieciowy	2
2.	Zarządzalny przełącznik sieciowy (typ 1)	1
3.	Zarządzalny przełącznik sieciowy (typ 2)	2
4.	Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych	1
5.	Serwer	2
6.	Macierz dyskowa	1
7.	Oprogramowanie do wykonywania kopii zapasowych	3
8.	Network Attached Storage - NAS	1
9.	UPS – zasilacz awaryjny UPS rack (typ 1)	1
10.	UPS – zasilacz awaryjny UPS rack (typ 2)	1
11.	UPS – zasilacze awaryjne UPS do stanowisk komputerowych	20
12.	Oprogramowanie typu EDR Endpoint Detection and Response	1

Kody CPV

- 48820000-2 Serwery
- 30233000-1 Urządzenie do przechowywania i odczytu danych
- 35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa
- 32420000-3 Urządzenie sieciowe
- 31682530-4 Awaryjne urządzenia energetyczne
- 48000000-8 Pakiety oprogramowania i systemy informatyczne
- 48422000-2 Zestawy pakietów oprogramowania
- 48600000-4 Pakiety oprogramowania dla baz danych i operacyjne



- 48900000-7 Różne pakiety oprogramowania i systemy komputerowe

1. Firewall sieciowy

Obszar wymagań	Wymagania minimalne
Wymagania ogólne	<p>Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.</p> <p>System realizujący funkcję firewall musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>System musi wspierać IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"> 1. Dla funkcji: firewall, IPSec, kontrola aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster active-active lub active-passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN.
Interfejsy, przestrzeń dyskowa	<ol style="list-style-type: none"> 1. System realizujący funkcję firewall musi dysponować minimum 7 portami Gigabit Ethernet RJ-45. 2. System firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
Wydajność	<ol style="list-style-type: none"> 1. W zakresie firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość stateful firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość firewall z włączoną funkcją kontroli aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.



	<ol style="list-style-type: none">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.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, kontrola aplikacji, antywirus - minimum 700 Mbps.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.
Funkcje systemu bezpieczeństwa	<p>W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none">1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.2. Kontrola Aplikacji.3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.5. Ochrona przed atakami - Intrusion Prevention System.6. Kontrola stron WWW.7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.8. Zarządzanie pasmem (QoS, Traffic shaping).9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system



Polityki firewall	<ol style="list-style-type: none">1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:<ul style="list-style-type: none">• Translację jeden do jeden oraz jeden do wielu.• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hashe złośliwych plików.
Połączenia VPN	<ol style="list-style-type: none">1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:<ul style="list-style-type: none">• Wsparcie dla IKE v1 oraz v2.• Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).• Obsługa protokołu Diffie-Hellman grup 19 i 20.• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.• Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.• Mechanizm „Split tunneling” dla połączeń Client-to-Site.2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:<ul style="list-style-type: none">• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.



	<ul style="list-style-type: none">• Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec VPN lub SSL VPN.
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie powinno zapewniać obsługę:</p> <ul style="list-style-type: none">• Routingu statycznego.• Policy Based Routingu.• Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
Funkcje SD-WAN	<ol style="list-style-type: none">1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
Zarządzanie pasmem	<ol style="list-style-type: none">1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	<ol style="list-style-type: none">1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.



Ochrona przed atakami	<ol style="list-style-type: none">1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	<ol style="list-style-type: none">1. Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.3. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.4. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	<ol style="list-style-type: none">1. Moduł kontroli WWW musi korzystać z bazy adresów URL pogrupowanych w kategorie tematyczne.2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.



	<ol style="list-style-type: none">5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none">1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:<ul style="list-style-type: none">• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	<ol style="list-style-type: none">1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3



	<p>oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.</p> <ol style="list-style-type: none">5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
Logowanie	<ol style="list-style-type: none">1. W ramach logowania system pełniący funkcję firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.3. Musi istnieć możliwość logowania do serwera SYSLOG.
Pozostałe wymagania	<p>W okresie obowiązywania gwarancji wszystkie funkcje bezpieczeństwa realizowane przez urządzenie muszą być dostępne bezpłatnie dla Zamawiającego, bez konieczności zakupu dodatkowych usług czy licencji subskrypcyjnych co najmniej w zakresie:</p> <p>kontrola aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), analiza typu Sandbox, antyspam, web filtering, bazy reputacyjne adresów IP/domen.</p>
Gwarancja	<p>Co najmniej 24-miesięczna gwarancja producenta.</p> <p>Wymagane warunki świadczenia serwisu gwarancyjnego:</p> <ul style="list-style-type: none">• usługi serwisu gwarancyjnego w miejscu instalacji urządzenia,• czas reakcji serwisu - do końca następnego dnia roboczego.



2. Zarządzalny przełącznik sieciowy (typ 1)

Obszar wymagań	Wymagania minimalne
Porty	Co najmniej: 24 porty 10/100/1000BASE-T umieszczone z przodu obudowy, 4 porty 1/10 Gb SFP+ umieszczone z przodu obudowy, wyposażone w moduły jednomodowe, 10Gps, złącze LC (po 1 module do każdego z 4 portów), dedykowany port konsoli USB, port USB 2.0 (niezależny od portu konsoli USB)
Wydajność	Przepustowość co najmniej 128 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika), wydajność co najmniej 95 Mp/s, bufor pakietów co najmniej 12 MB
Pamięć	Co najmniej 4 GB pamięci operacyjnej, co najmniej 16 GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash)
Tablice i obsługa ruchu	Tablica routingu co najmniej 500 wpisów IPv4 i 500 wpisów IPv6, tablica ARP co najmniej 1000 wpisów, tablica ND co najmniej 500 wpisów, tablica adresów MAC co najmniej 8000 pozycji, obsługa Jumbo Frames co najmniej 9198 bajtów
Monitorowanie i zarządzanie	Obsługa sFlow lub Netflow, obsługa REST API, obsługa RMON (co najmniej grupy 1,2,3 i 9), dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne
Obsługa sieci i protokołów	Obsługa 4094 tagów IEEE 802.1Q oraz 512 jednoczesnych sieci VLAN, obsługa protokołu MVRP, obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s), obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP), obsługa SNTPv4 lub NTP, wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping), obsługa routingu statycznego,



	obsługa ruchu multicast: IGMPv1/v2/v3 (co najmniej 500 grup), MLD (co najmniej 500 grup)
Zarządzanie urządzeniami końcowymi	Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED), automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED)
Mechanizmy QoS i optymalizacja ruchu	Mechanizmy zapewnienia jakości usług: priorytetyzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting
Uwierzytelnianie i autoryzacja dostępu	Obsługa uwierzytelniania zgodna z 802.1x, uwierzytelnianie użytkowników w oparciu o adres MAC i serwer RADIUS, uwierzytelnianie przez stronę WWW z użyciem zewnętrznego serwera, obsługa uwierzytelniania wielu użytkowników na tym samym porcie jednocześnie, obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+, obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+
Bezpieczeństwo i ochrona infrastruktury	Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD) lub równoważnego, ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection), obsługa list kontroli dostępu (ACL)
Obudowa	Przełącznik w obudowie do montażu w szafie rack 19", maksymalna wysokość obudowy 1U
Zasilanie	Wewnętrzny zasilacz 230V, pobór mocy nie większy niż 35W
Licencjonowanie	Jeżeli do działania którejkolwiek z wymaganych funkcji potrzebna jest licencja, należy ją dostarczyć. Wszystkie dostępne na przełączniku funkcje muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji o ile nie wyspecyfikowano inaczej.
Gwarancja	Tzw. dożywotnia gwarancja producenta (rozumiana jako co najmniej 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona



	<p>krótsza niż 2 lata po dostarczeniu sprzętu), obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do pomocy technicznej oraz poprawek i aktualizacji oprogramowania przez cały okres trwania gwarancji. Możliwość korzystania przez Zamawiającego z serwisu świadczonego bezpośrednio przez producenta sprzętu i komunikowania się bezpośrednio pomiędzy Zamawiającym i producentem sprzętu.</p>
--	--

3. Zarządzalny przełącznik sieciowy (typ 2)

Obszar wymagań	Wymagania minimalne
Porty	<p>Co najmniej: 48 portów 10/100/1000BASE-T umieszczone z przodu obudowy, 4 porty 1/10 Gb SFP+ umieszczone z przodu obudowy, wyposażone w moduły jednomodowe, 10Gps, złącze LC (po 1 module do każdego z 4 portów), dedykowany port konsoli USB, port USB 2.0 (niezależny od portu konsoli USB), dedykowany port do zarządzania poza pasmowego (RJ-45, Ethernet)</p>
Wydajność	<p>Przepustowość co najmniej 176Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika), wydajność co najmniej 130 Mp/s, bufor pakietów co najmniej 7.5 MB</p>
Pamięć	<p>Co najmniej 8 GB pamięci operacyjnej, co najmniej 15 GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash)</p>
Tablice i obsługa ruchu	<p>Tablica routingu co najmniej 2000 wpisów IPv4 i 1000 wpisów IPv6, tablica ARP co najmniej 8000 wpisów, tablica ND co najmniej 8000 wpisów, tablica adresów MAC co najmniej 16000 pozycji, obsługa Jumbo Frames co najmniej 9198 bajtów</p>
Łączenie w stos	<p>Przełączniki muszą obsługiwać łączenie w stos (wirtualny przełącznik) z minimum 8 urządzeń.</p>



	Zarządzanie jednym adresem IP, realizacja stosów na odległość co najmniej 300 m.
Monitorowanie i zarządzanie	Obsługa sFlow lub Netflow, obsługa REST API, obsługa RMON (co najmniej grupy 1,2,3 i 9), dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne, obsługa skryptów w języku Python. Zarządzanie przez interfejs Bluetooth (może być w formie adaptera USB od tego samego producenta). Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty.
Obsługa sieci i protokołów	Obsługa 4094 tagów IEEE 802.1Q oraz 2000 jednoczesnych sieci VLAN, obsługa standardu IEEE 802.1v, obsługa VXLAN, obsługa protokołu MVRP, obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s), obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP), obsługa SNTPv4 lub NTP, wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping), obsługa routingu statycznego, obsługa OSPF i OSPFv3, obsługa ruchu multicast: IGMPv1/v2/v3 (co najmniej 500 grup), MLD (co najmniej 1000 grup)
Zarządzanie urządzeniami końcowymi	Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED), automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED)



Mechanizmy QoS i optymalizacja ruchu	Mechanizmy zapewnienia jakości usług: priorytetyzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting
Uwierzytelnianie i autoryzacja dostępu	Obsługa uwierzytelniania zgodna z 802.1x, uwierzytelnianie użytkowników w oparciu o adres MAC i serwer RADIUS, uwierzytelnianie przez stronę WWW z użyciem zewnętrznego serwera, obsługa uwierzytelniania wielu użytkowników na tym samym porcie jednocześnie, obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+, obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+, wbudowany serwer DHCP, obsługa blokowania nieautoryzowanych serwerów DHCP.
Bezpieczeństwo i ochrona infrastruktury	Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD) lub równoważnego, ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection), obsługa list kontroli dostępu (ACL)
Obudowa	Przetątnik w obudowie do montażu w szafie rack 19", maksymalna wysokość obudowy 1U
Zasilanie	Wewnętrzny zasilacz 230V, pobór mocy nie większy niż 70W
Licencjonowanie	Jeżeli do działania którejkolwiek z wymaganych funkcji potrzebna jest licencja, należy ją dostarczyć. Wszystkie dostępne na przetątniku funkcje muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji o ile nie wyspecyfikowano inaczej.
Wyposażenie	Wraz z przetątnikami należy dostarczyć akcesoria umożliwiające połączenie dostarczonych urządzeń: kartę sieciową do posiadanego przez Zamawiającego serwera Supermicro 745BTQ-R920B posiadającą 4 porty 10 GbE SFP+, 10 patchordów światłowodowych LC/LC 2 metry, 4 patchordy RJ45 1 metr kat.6, 2 patchordy RJ45 0,5 metra kat.6. 8 wkładek światłowodowych SFP+ 10GB (850 NM, 300M, LC)



	Podano ilości łączne dla całego zamówienia.
Gwarancja	Tzw. dożywotnia gwarancja producenta (rozumiana jako co najmniej 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu), obejmująca wszystkie elementy przetłaczniaka (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do pomocy technicznej oraz poprawek i aktualizacji oprogramowania przez cały okres trwania gwarancji. Możliwość korzystania przez Zamawiającego z serwisu świadczonego bezpośrednio przez producenta sprzętu i komunikowania się bezpośrednio pomiędzy Zamawiającym i producentem sprzętu.

4. Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych

Obszar wymagań	Wymagania minimalne
Licencja, wsparcie	<p>Dostarczone licencje na oprogramowanie muszą być bezterminowe.</p> <p>Dostarczone licencje na oprogramowanie muszą być dostarczone z 12 miesięcznym wsparciem producenta, liczonym od dnia odbioru.</p> <p>Obsługa serwisowa w zakresie obsługi błędów realizowana ma być z czasem reakcji 16 godzin roboczych oraz czasem naprawy 80 godzin roboczych. W ramach wsparcia wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.</p> <p>Dostarczone licencje na oprogramowanie muszą objąć co najmniej 30 stanowisk komputerowych z systemem klasy Microsoft Windows. Ponadto musi posiadać co najmniej 1 licencję dostępową do konsoli zarządzającej.</p> <p>Wymagane przeprowadzenie wdrożenia systemu, dopuszcza się realizację wdrożenia w trybie zdalnym. Wymagane przeprowadzenie szkolenia systemu, co najmniej 2 godziny, dopuszcza się realizację szkolenia w trybie zdalnym.</p>



<p>Wymagania ogólne dla oprogramowania</p>	<p>Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.</p> <p>Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej.</p> <p>Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.</p> <p>Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.</p> <p>Agent systemu nie może nasłuchiwać na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika.</p> <p>Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompiłowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.</p> <p>Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną pracę wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych.</p> <p>Oprogramowanie musi posiadać dodatkową autoryzację użytkownika konsoli zarządzającej za pomocą usługi Google Authenticator oraz Microsoft Authenticator.</p> <p>Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).</p> <p>Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przełogowania użytkownika konsoli systemu).</p> <p>Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.</p>
--	---



	<p>Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019</p> <p>Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.</p> <p>Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych .</p> <p>Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie wybranych jednostek organizacyjnych oraz typów zasobów poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko wynikowe obiekty.</p> <p>Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (*.exe), plików bibliotek współdzielonych (*.dll), plików sterowników (*.sys) oraz pakietów instalacyjnych oprogramowania (*.msi).</p> <p>Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.</p> <p>Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).</p> <p>Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.</p> <p>Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).</p> <p>Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.</p> <p>Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez</p>
--	---



	<p>ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.</p> <p>Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.</p> <p>Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.</p> <p>Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.</p> <p>Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.</p> <p>Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.</p> <p>Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień użytkownika, zainstalowana usługa systemowa, ostatnie uruchomienie systemu, obecność pliku EXE na dysku, predefiniowane atrybuty komputera (np. dostawca, numer faktury, data zakupu).</p> <p>Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych.</p> <p>Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.</p>
--	---



	<p>Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.</p> <p>Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.</p>
Inwentaryzacja konfiguracji komputerów	<p>Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.</p> <p>Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.</p> <p>Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.</p> <p>Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417</p> <p>Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.</p> <p>Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.</p> <p>Oprogramowanie musi umożliwiać analizę sprzętową:</p> <ul style="list-style-type: none">- płyty głównej w zakresie model, producent, nr. seryjny,- CPU w zakresie nazwy, modelu, producenta, częstotliwości,- HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,- RAM w zakresie wielkości pamięci,- karty sieciowej w zakresie model, adres IP, adres MAC,- karty graficznej w zakresie model. <p>Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.</p>



	<p>Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.</p> <p>Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.</p> <p>Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.</p> <p>Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.</p> <p>Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.</p> <p>Oprogramowanie musi umożliwiać odczyt urządzeń podłączonych do stanowiska komputerowego przez interfejs USB, z możliwością odczytania nazwy urządzenia, producenta, modelu oraz numeru seryjnego (o ile urządzenie dostarcza ww. informacji)</p> <p>Oprogramowanie musi umożliwiać globalną analizę urządzeń podłączonych do stanowisk komputerowych przez interfejs USB</p> <p>Oprogramowanie musi umożliwiać integrację z zewnętrzną usługą Dell API w celu automatycznego odczytania informacji na temat okresu gwarancji stanowiska komputerowego na podstawie odczytanego przez agenta identyfikatora (ServiceTag)</p> <p>Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera).</p>
Inwentaryzacja oprogramowania	<p>Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.</p> <p>Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.</p> <p>Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).</p> <p>Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.</p> <p>Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.</p>



	<p>Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.</p> <p>Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.</p> <p>Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.</p> <p>Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.</p> <p>Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji.</p>
Zarządzanie licencjami, audyt oprogramowania	<p>Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania</p> <p>Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych w procesie automatycznego audytu licencji (rozliczenie ilościowe).</p> <p>Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade.</p> <p>Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.</p> <p>Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.</p>
Automatyzacja	<p>Oprogramowanie musi umożliwiać zdalną instalację pakietów *.msi, plików *.cmd, *.bat, *.reg, *.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie</p>



	<p>okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.</p> <p>Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.</p> <p>Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.</p> <p>Oprogramowanie musi umożliwiać tworzenie dystrybucji zadań oraz polis dla wybranych stanowisk komputerowych poprzez interaktywny kreator (krok po kroku). Wybór odbiorców musi uwzględniać listę stanowisk, strukturę organizacyjną, strukturę lokalizacyjną oraz dynamiczne grupy stanowisk.</p> <p>Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności.</p> <p>Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.</p> <p>Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).</p> <p>Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).</p> <p>Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD.</p>
--	---



	<p>Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.</p> <p>Oprogramowanie musi umożliwiać uruchomienie na prawach administracyjnych pliku instalacyjnego EXE (z GUI) w sesji użytkownika z ograniczonymi uprawnieniami do instalacji aplikacji. Proces instalacji jest manualnie kontynuowany przez użytkownika.</p> <p>Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.</p> <p>Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:</p> <p>Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Windows 10 z pamięcią RAM>4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0)</p> <p>Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0)</p> <p>Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi</p> <p>Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Windows 10 w architekturze 32 bitowej, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y.</p> <p>Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego.</p> <p>W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych.</p>
--	--



	<p>Oprogramowanie musi umożliwić instalację oprogramowania z plików exe, które nie posiadają instalacji w trybie cichym poprzez automatyzację procesu manualnej instalacji (nagrywanie makr w zakresie wyborów typu zaznaczenie checkbox, wybór pozycji z listy, kliknięcie przycisku, wpisanie parametru/ścieżki itp.)</p> <p>Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji</p> <p>Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika</p> <p>Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera)</p> <p>Nagrywanie makr musi być realizowane przez wybranie/wskazanie elementu okna, na którym ma zostać wykonana akcja (np. kliknięcie, wprowadzenie tekstu, zaznaczenie)</p> <p>Oprogramowanie musi umożliwiać wysyłanie komunikatów (Windows Notification) do wskazanych stanowisk komputerowych (wybór manualny, wg struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej)</p> <p>Oprogramowanie musi umożliwiać wysyłanie komunikatów przed każdą zdefiniowaną akcją automatyzacji (np.: przed rozpoczęciem instalacji pakietu MSI, przed dystrybucją plików, przed uruchomieniem skryptu PowerShell)</p> <p>Oprogramowanie musi umożliwiać automatyzację procesu konfiguracji dowolnej aplikacji Windows w celu odtworzenia zapamiętanych akcji (makr) dla wskazanych stanowisk komputerowych.</p>
Monitoring sieci LAN	<p>Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony</p> <p>Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru.</p>



	<p>Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.</p> <p>Oprogramowanie musi umożliwiać z zdaną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.</p> <p>Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.</p> <p>Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.</p> <p>Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.</p> <p>Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.</p>
--	--

5. Serwer

Obszar wymagań	Wymagania minimalne
Obudowa	<p>Do montażu w szafie serwerowej 19", o wysokości maksymalnie 1U z możliwością instalacji co najmniej 8 dysków SAS/SATA/NVMe 2.5". Serwer musi posiadać możliwość rozbudowy o 2 dodatkowe wnęki dyskowe na dyski SAS/SATA/NVMe 2.5".</p> <p>Serwer wraz z kompletem szyn umożliwiających montaż w szafie rack i wysuwania w celach serwisowych oraz ramieniem na okablowanie.</p> <p>Możliwość dokupienia przedniego panelu zamykanego na klucz, chroniącego dyski przed nieuprawnionym wyjęciem.</p>
Procesor	<p>Zainstalowany jeden procesor 16 rdzeniowy, zgodny z architekturą x86/64 bity, uzyskujący wynik co najmniej 28 900 punktów w teście PassMark - CPU Mark według wyników dostępnych na stronie http://www.cpubenchmark.net 30 dni przed terminem składania ofert lub później.</p> <p>Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim.</p>



	Ze względu na licencje oprogramowania posiadane przez Zamawiającego, nie dopuszcza się zaoferowania serwera z inną ilością rdzeni.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. Co najmniej 2 aktywne sloty PCI-E x16 obsługujące karty FHFL. Możliwość rozbudowy o 1 dodatkowy slot PCI-E x16.
Pamięć	Co najmniej 128 GB RAM DDR4 RDIMM 3200MT/s, w modułach po 64 GB RAM.
Dyski	Zainstalowane 2 dyski serwerowe SSD Read-Intensive o pojemności co najmniej 960 GB każdy (dyski będą skonfigurowane w RAID 1). Zainstalowany sprzętowy kontroler RAID SAS/SATA umożliwiający skonfigurowanie poziomów RAID 0, 1, 10.
Interfejsy sieciowe	Zainstalowane i w pełni funkcjonalne interfejsy co najmniej: 1 x RJ-45 Ethernet management port, 4 porty 10Gb/s Ethernet w standardzie SFP+ wyposażone we wkładki optyczne 10Gb/s SFP+ Multimode.
Złącza zewnętrzne	Co najmniej 5 x USB 3.x, w tym co najmniej 1 port na przednim panelu obudowy. Co najmniej 1 x microUSB lub USB-C na przednim panelu obudowy. Co najmniej 1 x VGA. Złącze microUSB / USB-C na przednim panelu musi umożliwiać dostęp do modułu zarządzania serwerem przez komputer PC z systemem Windows lub urządzenia mobilne z systemem Android lub iOS. Powyższe porty USB, microUSB / USB-C oraz VGA nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
Karta graficzna	Zintegrowana karta graficzna umożliwiająca wyświetlanie w rozdzielczości co najmniej 1920x1200
Wentylatory	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo. Ilość zainstalowanych wentylatorów musi umożliwiać wydajne chłodzenie dla maksymalnej konfiguracji serwera (CPU, RAM, PCI-E, dyski, zasilacze).



Zasilanie	Co najmniej dwa identyczne zasilacze zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera, o mocy każdego zasilacza nie więcej niż 850W.
Bezpieczeństwo	Fabrycznie wbudowany czujnik otwarcia obudowy. Moduł TPM.
Diagnostyka	Serwer musi mieć możliwość wyposażenia w panel diagnostyczny (LCD) umieszczony z przodu obudowy serwera, umożliwiający: <ul style="list-style-type: none">• wyświetlenie podstawowych informacji o serwerze, w tym numer seryjny oraz wersja oprogramowania zarządzającego i BIOS,• wyświetlanie stanu i logów, dla pamięci RAM, procesorów, pamięci masowej, wentylatorów, czujników temperatury i zasilaczy,• przywracanie konta administratora,• wyświetlanie w czasie rzeczywistym temperatury wlotu powietrza do serwera,• wyświetlanie w czasie rzeczywistym temperatury procesorów,• konfigurowanie ustawień sieciowych modułu zarządzania.
Zarządzanie	Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port 1 Gigabit Ethernet RJ-45 i umożliwiająca: <ul style="list-style-type: none">• monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.),• monitorowanie w czasie rzeczywistym poboru prądu przez serwer,• zbieranie logów błędów hardware,• przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury,• montowanie wirtualnych napędów,• zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego,• wysyłanie zawiadomień drogą mailową i poprzez SNMP• wsparcia dla IPMI, SSH, Redfish,



	<ul style="list-style-type: none">• wsparcie dla funkcji screenshot BSOD (Blue Screen of Death) dla systemów Windows,• nadawanie ról użytkownikom,• możliwość wykonania aktualizacji oprogramowania do zarządzania serwerem, BIOS, zasilaczy, LCD.
Dodatkowe oprogramowanie do zarządzania i monitorowania	<p>Wraz ze serwerem dostarczone powinno być oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające zdalne zarządzanie grupami serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające co najmniej na:</p> <ul style="list-style-type: none">• włączenie, wyłączenie, restart, podgląd logów serwerów, sprawdzenie statusu sprzętu, przejęcie pełnej konsoli graficznej serwerów,• tworzenie szablonów instalacyjnych dla systemów operacyjnych,• tworzenie profili serwerów ze zdefiniowanymi parametrami BIOS, procesora/-ów, pamięci, kontrolera RAID które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów,• zdalne montowanie obrazów ISO pozwalające na uruchomienie z nich serwera,• aktualizacja sterowników i BIOS serwerów.• zbieranie statystyk zużycia energii dla wszystkich serwerów z możliwością graficznej prezentacji danych historycznych.
System operacyjny	<p>System operacyjny, kompatybilny z oferowanym serwerem, spełniający n.w. wymagania minimalne:</p> <ol style="list-style-type: none">1) Możliwość wykorzystania co najmniej 4 TB pamięci RAM w środowisku fizycznym.2) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.3) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.4) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.5) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.



	<p>Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.</p> <p>6) Wbudowane wsparcie instalacji i pracy na wolumenach, które:</p> <ul style="list-style-type: none">a) pozwalają na zmianę rozmiaru w czasie pracy systemu,b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). <p>7) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</p> <p>8) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET</p> <p>9) Wbudowana zaporą internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</p> <p>10) Dostępne dwa rodzaje graficznego interfejsu użytkownika:</p> <ul style="list-style-type: none">a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. <p>11) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,</p> <p>12) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.</p> <p>13) Mechanizmy logowania w oparciu o:</p> <ul style="list-style-type: none">a) login i hasło,b) karty z certyfikatami (smartcard),c) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), <p>14) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz</p>
--	--



	<p>narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.</p> <p>15) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).</p> <p>16) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</p> <p>17) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.</p> <p>18) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).</p> <p>19) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</p> <p>20) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:</p> <ul style="list-style-type: none">a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:<ul style="list-style-type: none">i) Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,ii) Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,iii) Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.iv) Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1 i wyższych.
--	---



	<ul style="list-style-type: none">c) Zdalna dystrybucja oprogramowania na stacje robocze.d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:<ul style="list-style-type: none">i) dystrybucję certyfikatów poprzez http,ii) konsolidację CA dla wielu lasów domeny,iii) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,iv) automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.f) Szyfrowanie plików i folderów.g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).h) Serwis udostępniania stron WWW.i) Wsparcie dla protokołu IP w wersji 6 (IPv6),j) Wsparcie dla algorytmów Suite B (RFC 4869),k) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows. <p>21) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.</p> <p>22) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).</p> <p>23) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</p> <p>24) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</p> <p>25) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</p> <p>26) Zorganizowany system szkoleń i dostępne materiały edukacyjne w języku polskim.</p>
--	---



	<p>Zaoferowana wraz z serwerem licencja na system operacyjny:</p> <ol style="list-style-type: none">1. musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta i pozwalała na legalne używanie na oferowanym serwerze,2. musi obejmować najnowszą wersję systemu dostępną na dzień składania ofert,3. musi uprawniać do zainstalowania czterech instancji wirtualnych tego serwerowego systemu operacyjnego na każdym serwerze będącym przedmiotem zamówienia,4. musi obejmować licencje dostępowe dla 20 użytkowników, jeśli takie licencje są wymagane przez producenta do dostępu do oprogramowania serwerowego (liczba łączna dla obydwu serwerów). <p>Do oferty należy załączyć potwierdzenie kompatybilności serwera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim).</p>
Gwarancja	<p>Co najmniej 36 miesięcy gwarancji producenta. Usługi serwisu gwarancyjnego świadczone w miejscu instalacji urządzenia. Przyjmowanie zgłoszeń w trybie 9 godzin na dobę 5 dni w tygodniu. Wymagany czas reakcji serwisu - do końca następnego dnia roboczego.</p> <p>W okresie gwarancji musi być zapewniona:</p> <ul style="list-style-type: none">możliwość pobierania najnowszego firmware,dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania. <p>Możliwość darmowego pobierania aktualizacji firmware i sterowników bezpośrednio ze strony producenta serwera po ustaniu wsparcia serwisowego.</p> <p>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p>



	<p>Wymagane dołączenie do oferty oświadczenia Producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego Producenta.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub Producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p>
--	--

6. Macierz dyskowa

Obszar wymagań	Wymagania minimalne
Typ urządzenia	Macierz dyskowa typu hybrydowego (obsługująca dyski SSD oraz HDD) zapewniająca dostęp blokowy oraz plikowy do udostępnionej przestrzeni.
Kontrolery	<ol style="list-style-type: none"> Co najmniej dwa kontrolery macierzowe pracujące w trybie Symmetrical Active-Active/Mesh Active-Active, to znaczy w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów w trybie bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing) nawet dla pojedynczego LUN. W przypadku zaoferowania większej ilości kontrolerów obciążenie ma być rozłożone proporcjonalnie na wszystkie kontrolery. Każdy z kontrolerów macierzy musi posiadać minimum 64GB pamięci podręcznej Cache. Pamięć Cache do zapisu musi być mirrorowana pomiędzy kontrolerami. Komunikacja pomiędzy dostarczonymi kontrolerami macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się w szczególności komunikacji z wykorzystaniem protokołów FC/Ethernet/Infiniband. Obszar pamięci cache przechowujący zapisy musi mieć podtrzymanie bateryjne na wypadek awarii zasilania elektrycznego macierzy. Baterie muszą podtrzymać zasilanie pamięci przez co najmniej 48 godzin. Na wypadek awarii zasilania elektrycznego macierzy dopuszcza się



	<p>zastosowanie rozwiązania w postaci zrzutu pamięci cache do pamięci nieulotnej typu flash wbudowanej w kontroler.</p> <p>6. Kontrolery muszą posiadać możliwość ich wymiany (w przypadku awarii lub planowych zadań utrzymaniowych) bez konieczności wyłączenia zasilania całego urządzenia. Macierz musi obsługiwać wymianę kontrolera bez utraty danych zapisanych na dyskach.</p> <p>7. Każdy z kontrolerów macierzy musi być wyposażony w minimum jeden procesor wykonany w technologii wielordzeniowej z minimum 18 rdzeniami.</p> <p>8. Kontrolery muszą obsługiwać dostęp do danych protokołami blokowymi FC oraz iSCSI oraz plikowymi NFS i CIFS.</p> <p>9. Możliwość rozbudowy do co najmniej 4 par kontrolerów dyskowych tworzących jedną logiczną macierz bez konieczności wymiany zaoferowanej pary kontrolerów. Rozbudowa nie może odbywać się poprzez wirtualizację (podłączanie macierzy przez wirtualizator zasobów dyskowych).</p>
Obsługa RAID	Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: 5, 6, 10 oraz RAID z odpornością na jednoczesną awarię aż 3 dysków w grupie RAID (potrójna parzystość).
Przestrzeń dyskowa	<p>Zamontowane:</p> <ul style="list-style-type: none">• co najmniej 6 dysków HDD o pojemności co najmniej 8 TB każdy, skonfigurowane w RAID 5,• co najmniej 4 dyski SSD o pojemności co najmniej 480 GB każdy skonfigurowane w RAID 5.
Funkcjonalności zarządzania danymi w macierzy dyskowej	<p>1. Oferowana macierz musi umożliwiać definiowanie wirtualnych woluminów logicznych, których pojemność może być większa niż rzeczywista fizyczna przestrzeń dyskowa (ang: „thin provisioning”).</p> <p>2. Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych i używanych przez Zamawiającego: Windows, VMware, RedHat Linux</p>



	<ol style="list-style-type: none">3. Macierz musi mieć wsparcie dla automatycznego, bez agenta, odzyskiwania bloków (space reclamation lub free space defragmentation).4. Macierz musi umożliwiać utworzenie pełnej fizycznej kopii LUN typu klon. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, wymagane jest ich dostarczenie wraz z macierzą.5. Rozwiązanie musi umożliwiać tworzenie grup spójności, które gwarantują spójne kopiowanie, odtwarzanie i odświeżanie wielu wolumenów naraz tj. tworzenie kopii zapasowej wielu LUNów jednocześnie.6. Macierz musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych) na poziomie całych woluminów logicznych lub jego fragmentów bez konieczności rekonfiguracji po stronie serwerów korzystających z woluminów logicznych. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, wymagane jest ich dostarczenie wraz z macierzą.7. Wymagana jest funkcjonalność wykonywania kopii wirtualnych typu snapshot. Dostarczana macierz musi mieć możliwość utworzenia minimum 250 kopii migawkowych dla pojedynczego wolumenu (LUN) oraz minimum 2000 łącznie dla całej macierzy. Dla zasobów plikowych macierz musi umożliwiać wykonywanie kopii migawkowych systemu plików z którego dane udostępniane są protokołem CIFS. Po wykonaniu kopii zmiany danych lub zapisy w systemie plików nie będą miały wpływu na dane kopii migawkowej. Musi istnieć możliwość zabezpieczenia kopii migawkowej woluminów LUN oraz systemów plików przed modyfikacją i usunięciem przez zadany okres czasu w celu ochrony danych przed ransomware. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, wymagane jest ich dostarczenie wraz z macierzą.8. Macierz musi mieć możliwość wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy różnymi typami macierzy dyskowych w ramach tej samej rodziny modelowej. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych
--	--



	<p>technologicznie dyskach stałych (SAS, SSD, NL-SAS). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, wymagane jest ich dostarczenie wraz z macierzą.</p> <p>9. Macierz musi umożliwiać uruchomienie replikacji synchronicznej z inną macierzą z tej samej rodziny i zapewniać – w przypadku awarii urządzenia w jednym ośrodku przełączenie między macierzami musi odbywać się w sposób automatyczny i transparenty (bez przerywania dostępu do danych) dla korzystających z macierzy hostów. Macierz musi posiadać dedykowane oprogramowanie wykrywające awarie w klastrze rozciągniętym i monitorujące jego pracę (tzw. świadek). Opisana powyżej obsługa awarii (przełączenie między macierzami) musi odbywać się w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z macierzy hostów. Opisana funkcjonalność musi integrować się z platformą wirtualizacyjną VMware ESX.</p> <p>Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, wymagane jest ich dostarczenie wraz z macierzą.</p> <p>10. Macierz musi umożliwiać rozbudowę o funkcjonalność kompresji i deduplikacji danych w trybach in-line dla danych blokowych.</p>
Udostępnianie i kontrola dostępu do danych w macierzy	<p>1. Kontrolery macierzy muszą zapewnić dostęp plikowy NAS wspierający udostępnianie danych protokołami NFSv3, NFS4.0, CIFS, FTP, HTTPS.</p> <p>2. Uwierzytelnienie użytkowników za pomocą LDAP i ActiveDirectory</p> <p>3. Limity dyskowe (disk quota) zapewniające możliwość ustalania limitów dla przechowywanych danych dla wybranych użytkowników lub grup użytkowników (bez wykorzystania oprogramowania firm trzecich).</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z macierzą.</p>
Zarządzanie zasobami macierzy i jej konfiguracją	<p>1. Macierz musi posiadać oprogramowanie do zarządzania z graficznym interfejsem oraz znakowym (CLI) do monitorowania stanu i konfiguracji macierzy, diagnostyki, mapowania zasobów do serwerów. Dostęp do urządzenia</p>



	<p>bezpośrednio z poziomu standardowych przeglądarek internetowych oraz klientów SSH.</p> <ol style="list-style-type: none"> 2. Macierz musi być widoczna i zarządzana z poziomu jednej konsoli GUI. 3. Interfejs GUI musi umożliwiać monitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, woluminów logicznych LUN, oraz kontrolerów. 4. Możliwość konfigurowania woluminów logicznych LUN o pojemności użytkowej co najmniej 100 TB. 5. Macierz musi umożliwiać wykonywanie aktualizacji mikro kodu (firmware) macierzy w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji. <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z macierzą.</p>
Gwarancja	<p>Co najmniej 36 miesięcy gwarancji producenta. Wymagany czas reakcji serwisu - do końca następnego dnia roboczego.</p> <p>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p> <p>Wymagane dołączenie do oferty oświadczenia Producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego Producenta.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub Producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p>

7. Oprogramowanie do wykonywania kopii zapasowych

Obszar wymagań	Wymagania minimalne
Licencja	Wymagane dostarczenie licencji wieczystej zapewniającej ochronę 3 serwerów fizycznych oraz do korzystania ze wsparcia producenta przez okres 12 miesięcy.
Wymagania ogólne	Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter.



	<p>Oprogramowanie musi współpracować z infrastrukturą VMware oraz Microsoft Hyper-V. Wszystkie niżej wskazane funkcjonalności muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba że wyszczególniono inaczej</p> <p>Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.</p>
Wymagania szczegółowe	<p>Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.</p> <p>Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.</p> <p>Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.</p> <p>Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.</p> <p>Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych takiej puli.</p> <p>Oprogramowanie musi wspierać niezmiennność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.</p> <p>Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.</p> <p>Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn i</p>



	<p>baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time).</p> <p>Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.</p> <p>Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.</p> <p>Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.</p> <p>Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiegokolwiek funkcjonalności wymienionej w tej specyfikacji</p> <p>Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.</p> <p>Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.</p> <p>Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.</p>
Wymagania RPO	<p>Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.</p> <p>Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.</p> <p>Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru.</p> <p>Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych.</p> <p>Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.</p>



	<p>Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.</p> <p>Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.</p> <p>Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).</p> <p>Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi – wymagane co najmniej wsparcie dla serwera kopii zapasowych – deduplikatora danych będącego przedmiotem zamówienia.</p> <p>Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.</p> <p>Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.</p> <p>Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.</p> <p>Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.</p> <p>Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik</p> <p>Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)</p> <p>Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)</p>
Wymagania RTO	<p>Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i</p>



	<p>skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk Vmware i Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.</p> <p>Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).</p> <p>Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.</p> <p>Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.</p> <p>Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu.</p> <p>Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.</p> <p>Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.</p> <p>Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.</p> <p>Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.</p> <p>Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows i Linux.</p> <p>Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.</p>
--	--



	<p>Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI.</p> <p>Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.</p>
Wymagania ograniczenia ryzyka	<p>Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)</p> <p>Dla VMware oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.</p> <p>Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku.</p> <p>Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.</p> <p>Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem</p>



	<p>jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla ESET Endpoint Antivirus.</p> <p>Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.</p>
Wymagania dla agenta	<p>Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.</p> <p>Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych.</p> <p>Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu.</p> <p>Rozwiązanie musi wspierać system operacyjny macOS.</p> <p>Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux.</p> <p>Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą).</p> <p>Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster.</p> <p>Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów.</p> <p>Rozwiązanie musi wspierać backup podłączonych dysków USB. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym.</p> <p>Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury).</p> <p>Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone.</p> <p>Rozwiązanie musi wspierać kontrolę pasma sieciowego.</p>



	<p>Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych.</p> <p>Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN.</p> <p>Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft.</p> <p>Rozwiązanie musi wspierać technologię BitLocker.</p> <p>Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania.</p> <p>Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Active Directory, Microsoft SQL.</p> <p>Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych</p> <p>Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.</p> <p>Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere i Hyper-V.</p> <p>Rozwiązanie musi wspierać szyfrowanie.</p> <p>Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne.</p> <p>Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego.</p> <p>Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej.</p> <p>Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.</p>
Monitoring	<p>System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich</p>



	<p>System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Vmware – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie</p> <p>System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.</p> <p>System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter</p> <p>System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn</p> <p>System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel</p> <p>System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk</p> <p>System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora</p> <p>System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów</p> <p>System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)</p> <p>System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna</p> <p>System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego</p> <p>System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta</p> <p>System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.</p>
--	--



	<p>System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.</p>
Raportowanie	<p>System musi umożliwiać raportowanie środowiska wirtualizacyjnego Vmware – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie</p> <p>System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V zarówno w wersji darmowej, jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.</p> <p>System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.</p> <p>System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V</p> <p>System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF</p> <p>System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc</p> <p>System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach</p> <p>System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów</p> <p>System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych</p>



	<p>System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych</p> <p>System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury</p> <p>System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta</p> <p>System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.</p> <p>System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach „what-if”.</p> <p>System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware</p> <p>System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)</p> <p>System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.</p>
--	--

8. Network Attached Storage – NAS

Obszar wymagań	Wymagania minimalne
Budowa	Obudowa przystosowana do montażu w szafie rack 19” zajmująca maksymalnie 1U, wraz z szynami montażowymi Redundantne wentylatory
Procesor	Wielordzeniowy procesor 64-bitowy, uzyskujący wynik co najmniej 1000 punktów w teście PassMark - CPU Mark według wyników dostępnych na stronie http://www.cpubenchmark.net 30 dni przed terminem składania ofert lub później. Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim.
Pamięć RAM	Zainstalowane co najmniej 2 GB pamięci RAM, możliwość rozszerzenia do co najmniej 16 GB pamięci RAM.
Obsługa dysków	Ilość kieszeni dysków: co najmniej 4.



	<p>Obsługiwane typy dysków: Obsługa dysków hot-plug: 3,5" SATA, 2,5" SATA SSD</p> <p>Możliwość podłączenia modułu rozszerzającego</p>
Zamontowane dyski	<p>Zamontowane co najmniej 4 dyski o pojemności co najmniej 8 TB każdy, o prędkości interfejsu co najmniej 6Gbps i deklarowanym średnim czasem bezawaryjnej pracy co najmniej 1 mln godzin.</p> <p>Oferowane dyski muszą znajdować się na liście kompatybilności producenta urządzenia dyskowego NAS.</p>
Zarządzanie i bezpieczeństwo danych	<p>Obsługiwane systemy plików: EXT4 (wewnętrzne), EXT3, EXT4, NTFS, FAT32, HFS+ (zewnętrzne)</p> <p>Szyfrowanie wolumenów i dysków zewnętrznych (AES 256)</p> <p>Obsługa RAID (0, 1, 5, 6, 10, JBOD) i Hot Spare</p> <p>Monitorowanie S.M.A.R.T., skanowanie uszkodzonych bloków, odzyskiwanie RAID</p> <p>Obsługa migawek i replikacji migawek</p> <p>Obsługa mechanizmów backupu na zewnętrzne dyski</p>
Zarządzanie dostępem i użytkownikami	<p>Logowanie użytkowników przez CIFS/SMB, AFP, FTP, LDAP</p> <p>Integracja z Active Directory</p> <p>Ograniczanie dostępnej przestrzeni użytkowników (disk quota)</p> <p>Zarządzanie kontami i grupami użytkowników</p> <p>Obsługa zaawansowanych uprawnień (Windows ACL)</p>
Zarządzanie i monitorowanie systemu	<p>GUI i CLI do zarządzania macierzą</p> <p>Monitorowanie wydajności (I/O, przepustowość)</p> <p>Aktualizacje firmware w trybie online</p> <p>Powiadomienia przez e-mail/SMS</p> <p>Monitorowanie zasobów i rejestr zdarzeń</p> <p>Obsługa UPS</p>
Dostęp sieciowy i usługi NAS	<p>Serwer plików (CIFS/SMB, NFS, FTP, HTTPS)</p> <p>Obsługa iSCSI (Multi-LUN, LUN Mapping, MPIO)</p> <p>VPN (PPTP, OpenVPN)</p> <p>DDNS i zdalny dostęp</p> <p>Integracja z Google Drive, Dropbox, OneDrive</p>
Aplikacje i dodatkowe funkcje	<p>Aplikacje mobilne (zarządzanie, monitoring, obsługa kamer)</p> <p>Obsługa kontenerów LXD i Docker</p> <p>Obsługa serwera multimedialnego UPnP</p> <p>Obsługa serwera kopii zapasowych</p>
Porty	<p>Co najmniej 2 porty 2,5 GbE Base-T</p> <p>Co najmniej 2 porty 10 GbE SFP+</p>



	Co najmniej 4 porty USB 3.x Co najmniej 1 port PCIe
Zasilanie	Wbudowany zasilacz o mocy maksymalnej nie przekraczającej 250W
Gwarancja	Gwarancja producenta co najmniej 36 miesięcy.

9. UPS – zasilacz awaryjny UPS rack (typ 1)

Obszar wymagań	Wymagania minimalne
Typ urządzenia	Zasilacz awaryjny w obudowie typu tower z możliwością montażu w szafie rack, zajmujący maksymalnie 2U Wymagany zestaw do montażu w szafie rack
Moc	Co najmniej 3000 W, moc pozorna co najmniej 3000 VA
Topologia	On-line, VFI
Typ przebiegu	Sinusoida
Czas podtrzymania	10 min. dla obciążenia 50% lub dłużej 3,5 min. dla obciążenia 100% lub dłużej Możliwość podłączenia zewnętrznych modułów bateryjnych
Gniazda wyjściowe	Co najmniej: 4x IEC320 C13 (10A) sterowalne 4x IEC320 C13 (10A) 1x IEC320 C19 (16A)
Zabezpieczenia	Wyłącznik EPO NC Zabezpieczenie wejściowe: przeciwprzepięciowe, Przeciwzwarciovie - bezpiecznik automatyczny Zabezpieczenie wyjściowe: elektroniczne – przeciwzwarciovie i przeciążeniowe Zabezpieczenia wejścia DC (akumulatory wewnętrzne): Zabezpieczenie nadprądowe
Komunikacja	Co najmniej: RS232, USB HID, styki bezpotencjałowe 1-wejście; 1-wyjście; karta SNMP (wymagana)
Sygnalizacja	Akustyczno-diodowa wyświetlacz LCD oraz diody sygnalizujące usterkę, pracę baterijną, pracę w trybie online, obejście bypass
Oprogramowanie	Wymagane dedykowane oprogramowanie producenta UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość



	<p>zamykania systemu na co najmniej 30 stanowiskach komputerowych w sieci;</p> <p>Kompatybilne z Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów;</p> <p>możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPS'ów w oprogramowaniu.</p> <p>Konfiguracja minimalnego poziomu naładowania baterii. UPS po rozładowaniu baterii przed samoczynnym załączeniem zasilania wyjść (po powrocie zasilania sieciowego) musi ładować baterie do tego poziomu. Parametr ten ma zastosowanie w przypadku, gdy załączenie zasilania wyjść może nastąpić tylko wtedy, gdy UPS zgromadzi niezbędny zapas energii na wypadek kolejnego zaniku.</p> <p>Uruchamianie poprzez Bypass - aktywacja tej funkcji ma powodować, że UPS zawsze przed załączeniem zasilania wyjść na kilka sekund załączy zasilanie poprzez Bypass i po chwili przełączy się w zasilanie wyjść poprzez falownik (normalny tryb pracy). Funkcja ta ma umożliwiać załączenie urządzeń o zwiększonym prądzie rozruchowym bez przeciążania falownika UPS.</p>
Gwarancja	Gwarancja producenta co najmniej 24 miesiące na elektronikę i 24 miesięcy na akumulatory. Serwis gwarancyjny świadczony w systemie <i>door to door</i> . Czas naprawy do 5 dni roboczych.

10. UPS – zasilacz awaryjny UPS rack (typ 2)

Obszar wymagań	Wymagania minimalne
Typ urządzenia	Zasilacz awaryjny w obudowie typu tower z możliwością montażu w szafie rack, zajmujący maksymalnie 2U Wymagany zestaw do montażu w szafie rack
Moc	Co najmniej 2000 W, moc pozorna co najmniej 2000 VA
Topologia	On-line, VFI
Typ przebiegu	Sinusoida
Czas podtrzymania	16 min. dla obciążenia 50% lub dłużej 6 min. dla obciążenia 100% lub dłużej Możliwość podłączenia zewnętrznych modułów bateryjnych
Gniazda wyjściowe	Co najmniej:



	4x IEC320 C13 (10A) sterowalne 4x IEC320 C13 (10A)
Zabezpieczenia	Wyłącznik EPO NC Zabezpieczenie wejściowe: przeciwprzepięciowe, Przeciwzwarciove - bezpiecznik automatyczny Zabezpieczenie wyjściowe: elektroniczne – przeciwzwarciove i przeciążeniowe Zabezpieczenia wejścia DC (akumulatory wewnętrzne): Zabezpieczenie nadprądowe
Komunikacja	Co najmniej: RS232, USB HID, styki bezpotencjałowe 1-wejście; 1-wyjście; karta SNMP (wymagana)
Sygnalizacja	Akustyczno-diodowa wyświetlacz LCD oraz diody sygnalizujące usterkę, pracę baterijną, pracę w trybie online, obejście bypass
Oprogramowanie	<p>Wymagane dedykowane oprogramowanie producenta UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na co najmniej 30 stanowiskach komputerowych w sieci;</p> <p>Kompatybilne z Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów;</p> <p>możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPS'ów w oprogramowaniu.</p> <p>Konfiguracja minimalnego poziomu naładowania baterii. UPS po rozładowaniu baterii przed samoczynnym załączeniem zasilania wyjść (po powrocie zasilania sieciowego) musi ładować baterie do tego poziomu. Parametr ten ma zastosowanie w przypadku, gdy załączenie zasilania wyjść może nastąpić tylko wtedy, gdy UPS zgromadzi niezbędny zapas energii na wypadek kolejnego zaniku.</p> <p>Uruchamianie poprzez Bypass - aktywacja tej funkcji ma powodować, że UPS zawsze przed załączeniem zasilania wyjść na kilka sekund załączy zasilanie poprzez Bypass i po chwili przełączy się w zasilanie wyjść poprzez falownik (normalny tryb pracy). Funkcja ta ma umożliwiać załączenie urządzeń o</p>



	zwiększonym prądzie rozruchowym bez przeciążania falownika UPS.
Gwarancja	Gwarancja producenta co najmniej 24 miesiące na elektronikę i 24 miesięcy na akumulatory. Serwis gwarancyjny świadczony w systemie <i>door to door</i> . Czas naprawy do 5 dni roboczych.

11. UPS – zasilacze awaryjne UPS do stanowisk komputerowych

Obszar wymagań	Wymagania minimalne
Typ urządzenia	Zasilacz awaryjny w obudowie typu desktop
Moc	Co najmniej 330W, moc pozorna co najmniej 550 VA
Topologia	Line interactive
Typ przebiegu	Schodkowa aproksymacja sinusoidy
Czas przełączania	Maksymalnie 6 ms
Czas podtrzymania	6 min. dla obciążenia 50% lub dłużej 2 min. dla obciążenia 80% lub dłużej
Gniazda	Co najmniej: 1 gniazdo IEC320 C13 2 gniazda typu francuskiego.
Zabezpieczenia	Ochrona przeciwzwarciova Ochrona przeciwprzepięciowa Automatyczna regulacja napięcia (AVR)
Komunikacja	Co najmniej USB
Sygnalizacja	Sygnalizacja akustyczno-optyczna Dioda sygnalizująca minimum pracę sieciową, baterijną, niski poziom baterii, przeciążenie, awarię Sygnalizacja akustyczna informująca o minimum pracy bateryjnej, niskim poziomie baterii, przeciążeniu, awarii
Oprogramowanie	Jedno uniwersalne oprogramowanie do zarządzania oferowanymi urządzeniami UPS Oprogramowanie w języku polskim tego samego producenta co UPS do zarządzania i monitorowania pracy UPS . Wymagane wsparcie producenta (telefoniczne oraz e-mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. Możliwość edycji nazw urządzeń na liście monitorowanych UPSów Wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer



Gwarancja	Gwarancja producenta co najmniej 24 miesiące na elektronikę i 12 miesięcy na akumulatory
-----------	--

12. Oprogramowanie typu EDR Endpoint Detection and Response

Przedmiotem zamówienia jest rozbudowa aktualnie posiadanego oprogramowania antywirusowego o funkcje EDR lub, jako rozwiązanie równoważne, dostawa nowego oprogramowania spełniającego wymagania minimalne określone w tabeli poniżej.

Aktualnie Zamawiający posiada oprogramowanie ESET Protect Essential on-premise ilość licencji – 26 w tym serwer, licencje ważne do 29.06.2026.

Obszar wymagań	Wymagania minimalne
Licencja	Dostarczone licencje muszą zapewniać ochronę łącznie 26 urządzeń, w tym serwer, w Urzędzie Gminy Dzierzkowice przez okres 24 miesięcy.
Administracja zdalna w chmurze	<ol style="list-style-type: none"> 1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.



	<ol style="list-style-type: none">10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
Ochrona stacji roboczych	<ol style="list-style-type: none">1. Rozwiązanie musi wspierać systemy operacyjne Windows 10 i Windows 11.2. Rozwiązanie musi wspierać architekturę ARM64.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.



	<p>11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).</p> <p>12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.</p> <p>13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.</p> <p>14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, optycznych pamięci masowych, pamięci masowych FIREWIRE, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.</p> <p>15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.</p> <p>16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:</p> <ol style="list-style-type: none">tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi
--	---



	<p>samoczynnie przełączyć się w tryb pracy oparty na regułach,</p> <p>e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.</p> <p>17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.</p> <p>18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.</p> <p>19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p> <p>20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).</p> <p>21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.</p> <p>23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:</p> <ul style="list-style-type: none">a. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,b. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,c. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,d. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i
--	---



	<p>wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.</p> <p>24. Rozwiązanie musi być wyposażone w moduł bezpiecznej przeglądarki.</p> <p>25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez użytkownika.</p> <p>26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.</p> <p>27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.</p> <p>28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.</p> <p>29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.</p> <p>30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.</p>
Ochrona serwera	<p>1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2025, 2022 oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.</p> <p>2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.</p> <p>3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.</p> <p>4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.</p> <p>5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.</p> <p>6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p>



	<p>7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.</p> <p>8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.</p> <p>Dodatkowe wymagania dla ochrony serwerów Windows:</p> <p>9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.</p> <p>10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).</p> <p>11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.</p> <p>12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.</p> <p>14. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.</p> <p>15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.</p> <p>16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.</p> <p>17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.</p> <p>Dodatkowe wymagania dla ochrony serwerów Linux:</p> <p>18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.</p>
--	--



	<p>19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.</p> <p>20. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszzonego mikro-serwisu.</p>
Szyfrowanie	<ol style="list-style-type: none">1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).3. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
Ochrona urządzeń mobilnych opartych o system Android	<ol style="list-style-type: none">1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:<ol style="list-style-type: none">a. usunięcie zawartości urządzenia,b. przywrócenie urządzenia do ustawień fabrycznych,c. zablokowania urządzenia,d. uruchomienie sygnału dźwiękowego,e. lokalizację GPS.f. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.



	<ul style="list-style-type: none">g. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:h. nazwę aplikacji,i. nazwę pakietu,j. kategorię sklepu Google Play,k. uprawnienia aplikacji,l. pochodzenie aplikacji z nieznanego źródła.
Sandbox w chmurze	<ol style="list-style-type: none">1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.7. Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów.8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: Czysty, Podejrzany, Bardzo podejrzany, Szkodliwy.



	<p>13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.</p> <p>14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.</p> <p>15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.</p>
--	--