

Zamawiający:

Gmina Pieszyce

58-250 Pieszyce, ul. Tadeusza Kościuszki 1

NIP: 8821006077 REGON: 890717846

email: sekretariat@pieszyce.pl

tel.: 74 836 54 87

ZAŁĄCZNIK NR 1 DO SWZ

dla zamówienia publicznego o wartości nieprzekraczającej 1 024 799,00 złotych pod nazwą:

„Cyberbezpieczny Samorząd w Gminie Pieszyce”

OPIS PRZEDMIOTU ZAMÓWIENIA

Numer sprawy: SE.271.01.2026

Zamawiający informuje, że przedmiotem niniejszego zamówienia jest dostawa sprzętów i oprogramowania zgodnie z wytycznymi projektu Cyberbezpieczny Samorząd, a także usługa ich wdrożenia i konfiguracji, w tym w szczególności:

- dostawa centralnego systemu bezpieczeństwa, w tym urządzenia serwerowego, oprogramowania klasy SIEM, przełączników sieciowych, zarządzanych punktów dostępowych, oprogramowania do zarządzania infrastrukturą dla Urzędu Miasta i Gminy w Pieszcach;
- dostawa oprogramowania antywirusowego typu EDR do komputerów i innych urządzeń IT dla Urzędu Miasta i Gminy w Pieszcach;
- dostawa serwerów plików NAS wraz dyskami dla Urzędu Miasta i Gminy w Pieszcach oraz Jednostek Podległych;
- dostawa zasilaczy awaryjnych UPS typu rack dla Urzędu Miasta i Gminy w Pieszcach oraz Jednostek Podległych;
- dostawa routerów brzegowych dla Urzędu Miasta i Gminy w Pieszcach oraz Jednostek Podległych;
- dostawa oprogramowania do wykonywania kopii zapasowych dla Urzędu Miasta i Gminy w Pieszcach oraz Jednostek Podległych;
- usługa wdrożenia dostarczonych rozwiązań

- dostawa centralnego systemu bezpieczeństwa, w tym urządzenia serwerowego, oprogramowania klasy SIEM, przełączników sieciowych, zarządzanych punktów dostępowych, oprogramowania do zarządzania infrastrukturą dla Urzędu Miasta i Gminy w Pieszcach

a) Dostawa serwera na potrzeby uruchomienia aplikacji bezpieczeństwa

Przedmiotem niniejszego zamówienia jest dostawa serwera (1 sztuka) dla Urzędu Miasta i Gminy w Pieszcach.

Urządzenie musi być fabrycznie nowe, nieużywane, nierefabrykowane, wolne od wad fizycznych i prawnych oraz musi pochodzić z oficjalnego polskiego kanału dystrybucji. Urządzenie nie może być przedmiotem ekspozycji, testów ani pokazów.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ul style="list-style-type: none"> • Obudowa Rack o wysokości max 2U • 16 slotów na dyski 2.5" • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	<ul style="list-style-type: none"> • Płyta główna z możliwością zainstalowania jednego procesora. • Obsługa procesorów 144 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinny znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do 4TB pamięci RAM.
Chipset	<ul style="list-style-type: none"> • Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych.
Procesor	<ul style="list-style-type: none"> • Zainstalowany jeden procesor min. 16-rdzeniowy, min. 2.3GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 197 w teście SPECspeed2017_fp_base, dostępnym na stronie www.spec.org dla konfiguracji jednoprocessorowej oferowanego serwera.
RAM	<ul style="list-style-type: none"> • 64 GB DDR5 RDIMM 6400MT/s,
Kontroler RAID	<ul style="list-style-type: none"> – Sprzętowy kontroler dyskowy, posiadający <ul style="list-style-type: none"> ○ Min. 8GB nieulotnej pamięci cache, ○ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. ○ Wsparcie dla dysków samoszyfrujących ○ Obsługa dysków 24 Gbps SAS (SAS-4 / 22.5 Gbps) 12 Gbps SAS ,6 Gbps SAS/SATA, PCIe Gen 4 (NVMe)

Dyski twarde	<ul style="list-style-type: none"> – Zainstalowane: <ul style="list-style-type: none"> ○ 4x dysk SAS o pojemności min. 2.4TB, Hot-Plug ○ 2x dysk SSD o pojemności min. 480GB, Hot-Plug
Gniazda PCI	<ul style="list-style-type: none"> • Dwa sloty PCIe FH
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> – Wbudowane 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) – 1 moduł SFP+ SR 10 GbE
Wbudowane porty	<ul style="list-style-type: none"> • 4 porty USB w tym min: <ul style="list-style-type: none"> ○ 1 port USB 2.0 Type-C ○ 2 porty USB 3.1 ○ 1 port USB 3.0 wewnątrz obudowy • Port VGA z tyłu obudowy
Video	<ul style="list-style-type: none"> • Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	<ul style="list-style-type: none"> • Redundantne, Hot-Plug min. 1100W klasy Titanium
Elementy montażowe	<ul style="list-style-type: none"> – Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
System operacyjny/dodatkowe oprogramowanie	<ul style="list-style-type: none"> • Windows Server 2025 Standard – 40x Windows Server 2025/2022 User CALs
Bezpieczeństwo	<ul style="list-style-type: none"> – Zatrask górnej pokrywki oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. – Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. – Możliwość wyłączenia w BIOS funkcji przycisku zasilania. – BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła – Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. – Moduł TPM 2.0 V3 – Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera – Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem – Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami

	NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego spełnienie powyższych zaleceń.
Karta Zarządzania	<ul style="list-style-type: none"> – Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: <ul style="list-style-type: none"> ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej ○ szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika ○ możliwość podmontowania zdalnych wirtualnych napędów ○ wirtualną konsolę z dostępem do myszy, klawiatury ○ wsparcie dla IPv6 ○ wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer ○ integracja z Active Directory ○ możliwość obsługi przez sześciu administratorów jednocześnie ○ Wsparcie dla automatycznej rejestracji DNS ○ wsparcie dla LLDP ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej ○ możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. ○ Monitorowanie zużycia dysków SSD ○ Automatyczne zgłaszanie alertów do centrum serwisowego producenta ○ Automatyczne update firmware dla wszystkich komponentów serwera ○ Możliwość przywrócenia poprzednich wersji firmware ○ Możliwość eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON ○ Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych ○ Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. ○ Możliwość wykrywania odchyłeń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera ○ kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania ○ możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień

	<ul style="list-style-type: none"> o możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera o możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer o możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe <p>możliwość rozszerzenia funkcjonalności o:</p> <ul style="list-style-type: none"> o możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch o możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielokrotnego przy logowaniu do karty zarządzającej o Automatyczne odświeżanie certyfikatów SSL o monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	<ul style="list-style-type: none"> – Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych o integracja z Active Directory o Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta o Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish o Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram o Szczegółowy opis wykrytych systemów oraz ich komponentów o Możliwość eksportu raportu do CSV, HTML, XLS, PDF o Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. o Grupowanie urządzeń w oparciu o kryteria użytkownika o Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji o Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach o Szybki podgląd stanu środowiska o Podsumowanie stanu dla każdego urządzenia o Szczegółowy status urządzenia/elementu/komponentu o Generowanie alertów przy zmianie stanu urządzenia. o Filtry raportów umożliwiające podgląd najważniejszych zdarzeń o Integracja z service desk producenta dostarczonej platformy sprzętowej o Możliwość przejścia zdalnego pulpitu

- Możliwość podmontowania wirtualnego napędu
- Kreator umożliwiający dostosowanie akcji dla wybranych alertów
- Możliwość importu plików MIB
- Przesyłanie alertów „as-is” do innych konsol firm trzecich
- Możliwość definiowania ról administratorów
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
- Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
- Zdalne uruchamianie diagnostyki serwera.
- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
- Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin:
 - wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów
 - wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityką konfiguracji
 - z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)

	<ul style="list-style-type: none"> ▪ inwentaryzacja komponentów w serwerze i ich mikrokodów ▪ historia poboru mocy i temperatury serwera ▪ zbieranie danych diagnostycznych serwera do paczki serwisowej
Oprogramowanie do monitorowania	<p>Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT.</p> <p>Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <ul style="list-style-type: none"> – Monitoring: <ul style="list-style-type: none"> ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemu pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: <ul style="list-style-type: none"> ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliiach.

- Monitoring parametrów pamięci masowych z informacją o minimum:
 - Opóźnieniach
 - IOPS
 - Przepustowości
 - Utylizacji kontrolerów
 - Pojemność całkowita i dostępna
 - Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.
 - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
 - Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
 - Informacje o poziomie redukcji danych
 - Informacje o statusie replikacji oraz snapshotów
- Monitoring parametrów przełączników sieciowych z informacją o minimum:
 - Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
 - Stanie komponentów: zasilacze, wentylatory
 - Podłączonych hostach
 - Ilości i statusu portów
 - Utylizacji procesora
 - Utylizacji poszczególnych portów
 - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- Aktualizacja firmware
 - możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
 - możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania
- Raporty
 - Możliwość generowania raportów dla serwerów zawierających informację o:

	<ul style="list-style-type: none"> ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: <ul style="list-style-type: none"> ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF – Cyberbezpieczeństwo <ul style="list-style-type: none"> ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. – Wspierane urządzenia <ul style="list-style-type: none"> ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) – Wirtualny asystent <ul style="list-style-type: none"> ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; – Możliwość rozszerzenia funkcjonalności <ul style="list-style-type: none"> ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. – Inne <ul style="list-style-type: none"> ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	<ul style="list-style-type: none"> – Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 – Serwer musi posiadać deklaracja CE.

	<ul style="list-style-type: none"> – Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver, dla kraju, w którym produkt będzie użytkowany, według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. – Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
Dokumentacja użytkownika	<ul style="list-style-type: none"> – Zamawiający wymaga dokumentacji w języku polskim lub angielskim. – Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	<ul style="list-style-type: none"> – Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. – Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. – Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. – Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. – Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. – Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. – Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.

- Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
- Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
 - Możliwości utworzenia zgłoszenia serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
 - Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.
 - Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.
 - Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.
 - Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.
- Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

b) Dostawa systemu klasy SIEM do monitorowania bezpieczeństwa infrastruktury IT

1. Wymagania ogólne

1. Przedmiotem zamówienia jest dostawa, wdrożenie i konfiguracja centralnego systemu służącego do zbierania, agregowania, przechowywania i przeglądania logów z infrastruktury IT zamawiającego.
2. System ma umożliwiać bieżące gromadzenie logów z wybranych serwerów, stacji roboczych oraz urządzeń sieciowych.

3. Preferowane jest rozwiązanie oparte na technologii open-source, bez ograniczeń licencyjnych dotyczących liczby podłączonych źródeł logów i agentów.
4. Zamawiający udostępni zasoby w środowisku wirtualnym zgodnie z wymaganiami wykonawcy.
5. Wdrożenie może zostać zrealizowane zdalnie, przy użyciu bezpiecznych środków komunikacji, bez dodatkowych kosztów po stronie zamawiającego.

2. Wymagania funkcjonalne systemu

Oferowany system musi realizować co najmniej następujące funkcjonalności:

1. System musi umożliwiać centralne zbieranie logów z:
 - serwerów fizycznych i wirtualnych,
 - stacji roboczych,
 - usług katalogowych,
 - urządzeń sieciowych,
 - innych systemów i aplikacji przesyłających logi w standardowych formatach, w tym syslog.
2. System musi umożliwiać agregowanie logów w jednym miejscu oraz ich bezpieczne przechowywanie.
3. System musi umożliwiać podstawowe wyszukiwanie, filtrowanie i przeglądanie zgromadzonych logów.
4. System musi umożliwiać podstawowe alertowanie dla wybranych zdarzeń.
5. System musi zapewniać retencję logów przez okres co najmniej 24 miesięcy.
6. System musi posiadać standardowy interfejs webowy do obsługi administracyjnej i przeglądania danych.

c) Dostawa zarządzanych przełączników sieciowych

Przedmiotem niniejszego zamówienia jest dostawa 4 (czterech) sztuk fabrycznie nowych, wolnych od wad fizycznych i prawnych przełączników dostępowych warstwy 3 (switch).

Wszystkie oferowane urządzenia muszą być nieużywane, nierefabrykowane, a także nie mogły być przedmiotem ekspozycji, testów ani pokazów. Urządzenia muszą spełniać wszystkie parametry techniczne i wymagania określone w niniejszym dokumencie.

Lp.	Nazwa parametru	Wymagane parametry
1	Obudowa	Obudowa urządzenia musi być przystosowana do montażu w standardowej szafie 19” Maksymalne wymiary: Szerokość – 44,5 cm Głębokość – 27,5 cm Wysokość – 4,5 cm. Waga do 4 kg

2	Interfejsy	Minimum 48 gigabitowe interfejsy RJ-45 100/1000 Mbps, 2 interfejsy 100M/1G/2.5G/5G/10G Ethernet (RJ-45) 4 interfejsy 1G SFP/10G SFP+ Port konsoli USB-C
3	Wydajność	<ul style="list-style-type: none"> • Potencjał przełączania nie mniejszy niż 216 Gbps • Prędkość przełączania nie mniejsza niż 161 Mbps • Bufor pakietu nie mniejszy niż 2 Mbyte • Tabela adresów MAC nie mniejsza niż 32K • Jumbo frame (byte) – 9K • Flash nie mniej 64 MB • RAM nie mniej niż 1GB • L3 forwarding table - Max. 1 K IPv4 entries; Max. 512 IPv6 entries • Routing table - 64
4	Tryby pracy	<ul style="list-style-type: none"> • Urządzenie musi umożliwiać zdalną konfigurację i monitorowanie poprzez panel sterowania dostępny w technologii chmury, dostarczony bezpłatnie przez producenta urządzenia
5	Zgodność standardami	<ul style="list-style-type: none"> • IEEE 802.3z 1000BASE-X • IEEE 802.3ab 1000BASE-T Ethernet • IEEE 802.3an 10G BASE-T Ethernet • IEEE 802.3ae 10 Gbit/s Ethernet over fiber • IEEE 802.3az EEE • IEEE 802.3x flow control • IEEE 802.1AB LLDP/LLDP-MED • IEEE 802.1Q VLAN tagging • IEEE 802.1p Class of Service (CoS) prioritization • IEEE 802.1X port authentication
6	Odporność i dostępność	<ul style="list-style-type: none"> • IEEE 802.1D Spanning Tree Protocol (STP) • IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) • IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) • Static port trunking • IEEE 802.3ad LACP • Loop guard (with broadcast packet detection mechanism) • Root guard • BPDU guard • ErrDisable recovery • Dual configuration files • Dual images • ZULD • Flex link • Physical stacking • Flexible stacking
7	Kontrola ruchu	<ul style="list-style-type: none"> • 802.1Q static VLANs/dynamic VLANs: 4 K/4 K • Port-based VLAN • VLAN isolation • Vendor ID based VLAN • Protocol-based VLAN • IP subnet-based VLAN • MAC-based VLAN • Private VLAN • Voice VLAN

		<ul style="list-style-type: none"> • Independent VLAN Learning (IVL) • VLAN Translation • VLAN trunking • VLAN mapping • VLAN routing • IEEE 802.1AD VLAN stacking (QinQ) • VLAN ingress filtering • LACP algorithm of source/ destination IP or MAC • GVRP • L2PT
8	Bezpieczeństwo	<ul style="list-style-type: none"> • Port security • Layer 2 MAC filtering • Layer 3 IP filtering • Layer 4 TCP/UDP socket filtering • Static MAC forwarding • Multiple RADIUS servers • Multiple TACACS+ servers • 802.1x VLAN and 802.1p assignment by RADIUS • Login authentication by RADIUS • Login authentication by TACACS+ • TACACS+ accounting • RADIUS accounting • Authorization on RADIUS • Compound authentication • Authorization on TACACS+ • SSH v2 • SSL • MAC freeze • IP source guard (IPv4/IPv6) • DHCP snooping • DHCP Server Guard • ARP inspection • ARP freeze • Anti-ARP scan • Static IP-MAC-Port binding • Policy-based security filtering • Port isolation • MAC search • Guest VLAN • ACL packet filtering (IPv4/IPv6) • CPU protection • Interface related trap enable/disable (by port) • MAC-based authentication per VLAN • BPDU transparency • WoL/WoL Relay • Password encryption • Password complexity • Brute-force attack protection • SSH public key authentication

9	QoS	<ul style="list-style-type: none"> No. of hardware queues per port (Standalone/stacking): 8/6 Storm control and event log: Broadcast, multicast, unknown unicast (DLF) Port-based rate limiting (ingress/ egress) Rate limiting per IP/TCP/UDP per port Policy-based rate limiting 802.3x flow control 802.1p Class of Service (SPQ, WFQ, WRR, hybrid-SPQ combination capable) DiffServ (DSCP) Storm Control: Broadcast/Unknown Multicast/Unknown Unicast (DLF)
10	Layer 2 Multicast	<ul style="list-style-type: none"> L2 multicast IGMP snooping (v1, v2, v3) IGMP snooping fast leave IGMP snooping immediate leave Configurable IGMP snooping timer and priority IGMP snooping statistics IGMP throttling IGMP filtering IGMP proxy mode & snooping mode selection Multicast load balance over trunking port Static mulitcast MVR support MLD snooping (MLD v1/v2)
11	Routing	<ul style="list-style-type: none"> Static route IP port moving Policy-based route
12	Zarządzanie	<ul style="list-style-type: none"> SNMP v1, v2c, v3 SNMP trap group RMON (1, 2, 3, 9) ICMP echo/echo reply Syslog IEEE 802.1AB LLDP/LLDP-MED Custom default Syslog (IPv4/IPv6) Display port utilization DHCP relay per VLAN DHCP smart relay DHCP relay option 82 SSH Remote Command Execution
13	Zarządzanie IPv6	<ul style="list-style-type: none"> IPv6 over Ethernet (RFC 2464) IPv6 addressing architecture (RFC 4291) Dual stack (RFC 4213) ICMPv6 (RFC 4443) Path MTU (RFC 1981) Minimum path MTU size of 1280 (RFC 5095) Encapsulation for maximum PMTU of 1500 Neighbor discovery (RFC 4861) DHCPv6 snooping IPv6 binding- static/dynamic Extend Radius server DHCPv6 relay

		<ul style="list-style-type: none"> • Default DHCP client mode
14	Zarządzanie urządzeniem	<ul style="list-style-type: none"> • Standalone management by Web interface • Cloud management • Networked AV mode by Web Interface • Optimized Dante and AES67 in Networked AV mode • Intuitive Cloud connection status • Management through Console, Telnet, SNMP • Remote firmware upgrade by FTP/ Web/TFTP • Configuration saving and retrieving • Multiple logins supported • Configure clone • Custom default Configuration • Multilevel CLI • CLI (Cisco-like) • DHCP server • DHCP relay per VLAN • DHCP client IPv4/IPv6 • DHCP client option 60 • DHCP option 82 • Daylight saving • DHCP relay MAC proxy • Auto PD Recovery • NTP supports IPv4/IPv6 • Port mirroring • Policy-based mirroring • Mirror CPU • VLAN-based mirroring • USB-C out-of-band console port • Auto PD Recovery • LLDP power via MDI • sFlow • Fiber Module Rescue • SSH Remote Command Execution
15	MIB	<ul style="list-style-type: none"> • RFC 1066 TCP/IP-based MIB • RFC 1213, 1157 SNMPv2c/v3 MIB • RFC 1493, 4188 bridge MIB • RFC 1643 Ethernet MIB • RFC 1757 RMON group 1, 2, 3, 9 • RFC 2011, 2012, 2013 SNMPv2 MIB • RFC 2233 SMIv2 MIB • RFC 2358 Ethernet-like MIB • RFC 2674 bridge MIB extension • RFC 2819, 2925 remote management MIB • RFC 3621 power Ethernet MIB • RFC 4022 management information base for transmission control protocol • RFC 4113 management information base for user datagram protocol • RFC 4292 IP forwarding table MIB • RFC 4293 Management Information Base (MIB) for IP • Cable diagnostic MIB
16	Zakres temperaturowy pracy	-20°C do 50°C

17	Zasilanie	Maksymalna moc pobierana przez urządzenie nie może przekraczać 54W.
18	Ochrona przed wyładowaniami elektrostatycznymi/przepięciami	Zabezpieczenie przeciwprzepięciowe portu Ethernet – 2KV Ochrona zasilacza Linia-GND – 2KV Ochrona zasilacza Linia-Linia – 1KV Ochrona ESD portu Ethernet (powietrze/kontakt) - 8 KV/6 KV
19	Rozpraszanie ciepła (BTU/godz.)	195.43
20	Hałas akustyczny przy 25°C (min./maks., dBA)	27.0/49.95
21	MTBF (hr)	Parametr ten nie powinien być niższy niż 298,735
22	Gwarancja	Urządzenie powinno posiadać ograniczoną dożywnotną gwarancję producenta
23	Serwis	W przypadku awarii urządzenia, wysyłka zastępczego produktu następuje w następnym dniu roboczym, po którym zgłoszona zostanie awaria. Urządzenie powinno być objęte w/w opcją serwisową w okresie nie krótszym niż 5 lat.
24	Wymagane Certyfikaty	Bezpieczeństwo • LVD • BSMI EMC • FCC Part 15 (Class A) • CE EMC (Class A) • BSMI EMC RoHS • Level A
25	Pozostałe	Sprzęt musi być fabrycznie nowy i pochodzić z polskiego kanału dystrybucji

d) Dostawa zarządzanych punktów dostępowych (access point)

Przedmiotem niniejszego zamówienia jest dostawa 7 (siedmiu) sztuk fabrycznie nowych, wolnych od wad fizycznych i prawnych punktów dostępowych (access point).

Wszystkie oferowane urządzenia muszą być nieużywane, nierefabrykowane, a także nie mogły być przedmiotem ekspozycji, testów ani pokazów. Urządzenia muszą spełniać wszystkie parametry techniczne i wymagania określone w niniejszym dokumencie.

Lp.	Nazwa parametru	Wymagane parametry
1	Obudowa	Obudowa urządzenia musi być przystosowana do montażu do sufitowego
2	Ilość portów	Urządzenie w standardzie musi posiadać 2 porty 1/2.5 Gbps LAN
3	Tryb pracy	Urządzenie musi umożliwiać pracę w jednym z poniższych trybów: <ul style="list-style-type: none"> • samodzielny (standalone) • zdalną konfigurację i monitorowanie poprzez panel sterowania dostępny w technologii chmury, dostarczony bezpłatnie przez producenta urządzenia

4	Funkcje WLAN	<p>Urządzenie musi:</p> <ul style="list-style-type: none"> • posiadać co najmniej dwa radia • obsługiwać MU-MIMO • minimalny zysk anteny 1.49 dBi dla pasma 2,4Ghz (2x2: 2SS) • minimalny zysk anteny 2.78 dBi dla pasma 5Ghz (4x4: 4SS) • minimalny zysk anteny 3.17 dBi dla pasma 6Ghz (4x4: 4SS) • minimalna prędkość przesyłu danych: 688 Mbps dla pasma 2,4Ghz • minimalna prędkość przesyłu danych: 8646 Mbps dla pasma 5Ghz • minimalna prędkość przesyłu danych: 11530 Mbps dla pasma 6Ghz • obsługiwać Band Steering • obsługiwać WDS/Mesh • obsługiwać DCS i Load Ballancing • obsługiwać Fast Roaming (Pre-authentication, PMK caching and 802.11 r/k/v) • obsługiwać technologię advanced cellular coexistence
5	Bezpieczeństwo	<p>Urządzenie musi: wspierać:</p> <ul style="list-style-type: none"> • WEP • WPA • WPA2 • WPA3 • IEEE 802.1X • MAC filtering • L2 isolation • RADIUS authentication • Rogue AP detection
6	Funkcje sieci	<p>Urządzenie musi: wspierać:</p> <ul style="list-style-type: none"> • IPv6 • VLANs • WMM • U-APSD
7	Zarządzanie	<p>Urządzenie musi: wspierać zarządzanie poprzez:</p> <ul style="list-style-type: none"> • Web UI • CLI • SNMP • Cloud
8	Zasilanie	Punkt dostępowy musi umożliwiać jego zasilanie z PoE, Maksymalny pobór mocy nie może być większy niż 22 W
9	MTBF (hr)	Parametr ten nie powinien być niższy niż 691,722
10	Gwarancja	Urządzenie powinno być objęte ograniczoną dożywotnią gwarancją producenta
11	Serwis	W przypadku awarii urządzenia, wysyłka zastępczego produktu następuje następnego dnia roboczego po tym, w którym zgłoszona zostanie awaria. Urządzenie powinno być objęte w/w opcją serwisową w okresie nie krótszym niż 5 lat.
12	Wymagane Certyfikaty	Radio: FCC Part 15C, FCC Part 15E, FCC Part 2.1091, ETSI EN 300 328, EN 301 893, Draft EN 303 687, EN 50385, EN 50665, EN IEC 62311, LP0002

		EMC: FCC Part 15B, EN 301 489-1, EN 301 489-17, EN55032, EN55035, EN61000-3-2/-3, EN60601-1-2, BSMI CNS15936
		Bezpieczeństwo: EN 62368-1, IEC 62368-1, BSMI CNS15598-1
13	Pozostałe	Sprzęt musi być nowy i pochodzić z polskiego kanału dystrybucji

e) Dostawa oprogramowania do zarządzania infrastrukturą

Zamawiający wymaga dostarczenia rozwiązania obejmującego 64 stacji roboczych, które obejmuje wdrożenie, usługę szkoleniową oraz licencję bezterminową. Dodatkowo oczekuje się zapewnienia rocznego wsparcia technicznego producenta. Oferowane oprogramowanie powinno spełniać poniższe wymagania funkcjonalne:

Wymagania ogólne dla systemu zarządzania:

Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.
Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agent/Konsoli zarządzającej.
Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.
Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.
Agent systemu nie może nasłuchiwać na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika.
Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompiowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.
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.
Oprogramowanie musi posiadać dodatkową autoryzację użytkownika konsoli zarządzającej za pomocą usługi Google Authenticator oraz Microsoft Authenticator.
Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).
Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.
Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019
Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.
Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych.
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.
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).

Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.
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).
Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.
Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).
Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.
Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.
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.
Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.
Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.
Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.
Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.
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).
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.
Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.
Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.
Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.

Inwentaryzacja konfiguracji komputerów:

Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.
Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.
Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.

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
Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.
Oprogramowanie musi umożliwiać analizę sprzętową: <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.
Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.
Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.
Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.
Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.
Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.
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)
Oprogramowanie musi umożliwiać globalną analizę urządzeń podłączonych do stanowisk komputerowych przez interfejs USB
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)
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).

Inwentaryzacja oprogramowania:

Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.
Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.

Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.
Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.
Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.
Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji.

Zarządzanie licencjami, audyt oprogramowania:

Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania
Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych w procesie automatycznego audytu licencji (rozliczenie ilościowe).
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.
Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.
Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.

Zdalny pulpit, zdalne zarządzanie komputerem:

Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpitu nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy).
Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.
Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).
Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.
Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).
Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.
Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.
Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.
Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.

Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.
Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe
Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL
Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows
Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN
Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połączenie konsoli ze wskazanym serwerem aplikacji.
Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

Automatyzacja:

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 okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.
Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.
Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.
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.
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.
Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.
Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).
Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).
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.
Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.
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.

Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.

Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:

1. 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)
2. 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)
3. 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
4. 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.
5. Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego.

W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych.

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.)

Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji

Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika

Oprogramowanie musi wznowiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera)

Nagrywanie makr musi być realizowane przez wybranie/wskazanie elementu okna, na którym ma zostać wykonana akcja (np. kliknięcie, wprowadzenie tekstu, zaznaczenie)

Oprogramowanie musi umożliwiać wysyłanie komunikatów (Windows Notification) do wskazanych stanowisk komputerowych (wybór manualny, wg struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej)

Oprogramowanie musi umożliwiać wysyłanie komunikatów przed każdą zdefiniowaną akcją automatyzacji (np.: przed rozpoczęciem instalacji pakietu MSI, przed dystrybucją plików, przed uruchomieniem skryptu PowerShell)

Oprogramowanie musi umożliwiać automatyzację procesu konfiguracji dowolnej aplikacji Windows w celu odtworzenia zapamiętanych akcji (makr) dla wskazanych stanowisk komputerowych.

Backup danych użytkownika

Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.

Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).

Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. *.doc, które mają być archiwizowane.

Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.
Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)
Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji.
Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji.

Zarządzanie urządzeniami USB Storage:

Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny.
Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane.
Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USBStorage.
Oprogramowanie musi umożliwiać włączenie trybu ReadOnly dla klasy USBStorage
Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD

Monitoring stanowisk komputerowych:

Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.
Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.
Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).
Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach
Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego).
Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.
Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione.
Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności).
Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.
Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania
Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.
Oprogramowanie musi umożliwiać analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć).
Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP
Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB. Monitorowanie tych wydruków musi odbywać się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej.

Oprogramowanie po zainstalowaniu musi przysyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z którego dany sterownik korzysta, opis sterownika drukarki, format drukowanych stron oraz nazwę drukowanego dokumentu.

Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor).

Wymagania formalne:

Zamawiający wymaga dołączenia do oferty ważnego certyfikatu producenta potwierdzającego zgodność z normą ISO/IEC 27001:2022. Certyfikat musi obejmować działalność w zakresie produkcji, rozwoju oprogramowania, integracji systemów, zarządzania infrastrukturą IT, testów, usług servicedesk i inżynieryjnych, a także sprzedaży, projektowania, realizacji projektów, wdrażania, utrzymania i serwisu. Dokument musi być wystawiony przez akredytowaną jednostkę certyfikującą i potwierdzać spełnienie najwyższych standardów bezpieczeństwa informacji w obszarze realizacji usług i produktów objętych ofertą.

Zamawiający wymaga dołączenia do oferty ważnego certyfikatu potwierdzającego, że producent stosuje System Zarządzania Jakością zgodny z normą PN-EN ISO 9001:2015. Certyfikat musi obejmować działalność w zakresie usług informatycznych, takich jak produkcja, rozwój oprogramowania, integracja systemów, zarządzanie infrastrukturą IT, testy, usługi servicedesk i inżynieryjne, a także sprzedaż, projektowanie, realizacja projektów, wdrażanie, utrzymanie i serwis.

W okresie trwania umowy wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.

Obsługa serwisowa musi być realizowana przez Producenta oprogramowania, w dni robocze w godzinach 8-16 w języku polskim, zgodnie z poniższymi parametrami:

Typ zgłoszenia	Opis	Czas Reakcji (godziny robocze)	Czas Realizacji (godziny robocze)
Błąd Krytyczny	Nieprawidłowości, która uniemożliwia dalsze korzystanie z Systemu - awaria	2h	8h
Usterka Ważna	Nieprawidłowości utrudniające korzystanie z Systemu, ale w stopniu umożliwiającym dalsze korzystanie	8h	40h
Usterka	Nieprawidłowości utrudniająca korzystanie z Systemu, ale w stopniu umożliwiającym i nieutrudniającym w sposób znaczny dalsze korzystanie	16h	80h

Dostarczone licencje na oprogramowanie muszą objąć co najmniej 64 stanowisk komputerowych z systemem klasy Microsoft Windows, Licencje nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp). Ponadto musi posiadać co najmniej 1 licencji dostępowych do konsoli zarządzającej

W przypadku wątpliwości zamawiający zastrzega sobie prawo (w przeciągu do 7 dni od terminu otwarcia ofert) do wezwania wykonawcy do prezentacji zaoferowanego rozwiązania celem weryfikacji zgodności z wymaganiami stawianymi przez zamawiającego w niniejszym postępowaniu.

Zamawiający wymaga od wykonawcy, aby przeprowadził wdrożenie systemu w siedzibie zamawiającego/zdalnie (wymagana co najmniej 1 sesji – 2 godzin każda):

Zamawiający wymaga od wykonawcy, aby w terminie 30 dni od zakończenia prac wdrożeniowych przeprowadził szkolenie z obsługi systemu w siedzibie zamawiającego/zdalnie (wymagana co najmniej 1 sesje – 2 godzinne)

- dostawa oprogramowania antywirusowego typu EDR do komputerów i innych urządzeń IT dla Urzędu Miasta i Gminy w Pieszczykach oraz Jednostek Podległych

System antywirusowy z funkcjonalnością EDR oraz MDR – Cała funkcjonalność oprogramowania ma być zapewniona w formie licencji dla 60 użytkowników oraz 3 serwerów na okres do 30.06.2026 r.

Wymagania dla poszczególnych modułów:

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

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

Rozwiązanie dla ochrony antywirusowej stacji roboczych musi wspierać następujące systemy operacyjne:

- Microsoft Windows 10
- Microsoft Windows 11
- macOS version 14 "Sonoma"
- macOS version 13 "Ventura"
- macOS version 12 "Monterey"

Rozwiązanie dla ochrony antywirusowej systemów serwerowych musi wspierać następujące systemy operacyjne:

- Microsoft® Windows Server 2016 Standard
- Microsoft® Windows Server 2016 Essentials
- Microsoft® Windows Server 2016 Datacenter
- Microsoft® Windows Server 2016 Core
- Microsoft® Windows Server 2019 Standard
- Microsoft® Windows Server 2019 Essentials
- Microsoft® Windows Server 2019 Datacenter
- Microsoft® Windows Server 2019 Core
- Microsoft® Windows Server 2022 Standard
- Microsoft® Windows Server 2022 Essentials
- Microsoft® Windows Server 2022 Datacenter
- Microsoft® Windows Server 2022 Core

Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppe@cppe.gov.pl



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

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

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

Opis technologii

1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity.
2. Rozwiązanie musi posiadać wbudowany mechanizm ochrony przed zagrożeniami typu ransomware.
3. Rozwiązanie musi wspierać technologię Antimalware Scan Interface (AMSI)
4. Rozwiązanie musi umożliwiać wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
5. W momencie wykrycia infekcji rozwiązanie automatycznie musi starać się wyleczyć plik, a jeśli nie jest to możliwe to przenosić go do bezpiecznego folderu kwarantanny.
6. Rozwiązanie musi posiadać możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwalając na: musi wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
7. Rozwiązanie musi chronić plik systemowy HOSTS przed nieautoryzowanymi zmianami.
8. Rozwiązanie musi posiadać mechanizmy skanujące dyski sieciowe.
9. Skanowanie dysków sieciowych musi być możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
10. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
11. Rozwiązanie musi posiadać mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
12. Musi istnieć możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
13. Aktualizacje baz definicji wirusów muszą być dostępne 24h na dobę na serwerze internetowym producenta, umożliwiać zarówno aktualizację automatyczną programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
14. Uaktualnienia definicji wirusów muszą posiadać podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
15. Rozwiązanie musi posiadać możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
16. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, musi następować w sposób automatyczny, niewidoczny dla użytkownika końcowego.
17. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej ma nie wymagać dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następować automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.

18. Rozwiązanie musi posiadać możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.
19. Rozwiązanie musi posiadać możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
20. Rozwiązanie musi posiadać możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
21. Rozwiązanie musi posiadać możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
22. Rozwiązanie musi posiadać możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
23. Rozwiązanie musi posiadać możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
24. Rozwiązanie musi posiadać możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
25. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego.
26. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
27. Rozwiązanie musi posiadać funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
28. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
29. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
30. Rozwiązanie musi posiadać heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
31. Musi być umożliwione wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit”.
32. Wyposażenie w mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.
33. Rozwiązanie musi posiadać technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.
34. Rozwiązanie musi posiadać technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.
35. Rozwiązanie musi posiadać możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
36. Rozwiązanie musi posiadać możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.
37. Rozwiązanie musi posiadać możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
38. Rozwiązanie musi posiadać możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.

39. Rozwiązanie musi automatycznie powiadamiać użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
40. Rozwiązanie musi posiadać możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
41. Rozwiązanie musi posiadać możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
42. Rozwiązanie musi umożliwiać blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
43. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
44. Rozwiązanie musi posiadać możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.
45. Rozwiązanie musi być wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamianie skryptów ActiveX i pobierane pliki.
46. Rozwiązanie musi posiadać możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
47. Rozwiązanie musi umożliwiać blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
48. Oprogramowanie musi zapewniać co najmniej 30 kategorii klasyfikacji witryn WWW.
49. Użytkownik podczas próby przejścia na witrynę znajdującą się w zablokowanej przez Administratora kategorii, musi być powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
50. Rozwiązanie musi umożliwiać blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
51. Rozwiązanie musi posiadać wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.
52. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie musi blokować możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
53. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie musi automatycznie blokować zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.
54. Kontrola połączenia musi umożliwiać zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
55. Rozwiązanie musi posiadać wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
56. Rozwiązanie musi posiadać funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
57. Profile bezpieczeństwa zapory ogniowej muszą zawierać predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
58. Rozwiązanie musi pozwalać na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.
59. Rozwiązanie musi posiadać możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).

60. Rozwiązanie musi umożliwiać stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
61. Rozwiązanie musi być wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
62. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
63. Moduł aktualizacji aplikacji, okresowo ma skanować aplikacje zainstalowane na stacji roboczej i umożliwiać ich aktualizację do najnowszych wersji.
64. Moduł aktualizacji aplikacji musi pełnić rolę mechanizmu łąiącego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
65. Administrator musi posiadać możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
66. Administrator musi posiadać możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
67. Mechanizm aktualizacji aplikacji musi umożliwiać automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
68. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator musi posiadać możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.
69. Administrator konsoli zarządzającej musi posiadać możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
70. Mechanizm aktualizacji aplikacji (patch management) ma nie wymagać uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
71. Administrator musi mieć możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
72. Rozwiązanie musi umożliwiać wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
73. System centralnego zarządzania musi prezentować niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
74. Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
75. Mechanizm kontroli urządzeń zewnętrznych musi wspierać m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.
76. Oprogramowanie musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
77. Lista urządzeń zaufanych musi być tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
78. Rozwiązanie musi posiadać możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
79. Mechanizm kontroli urządzeń musi umożliwiać blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
80. Rozwiązanie musi posiadać opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.

81. Zmiany w konfiguracji mają być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
82. Rozwiązanie musi posiadać możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker
83. Rozwiązanie musi pozwalać na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.
84. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator musi posiadać możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.
85. Rozwiązanie musi pozwalać na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.
86. Administrator w konsoli zarządzającej musi posiadać dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.
87. Rozwiązanie musi posiadać wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.
88. Mechanizm w swoim działaniu musi wykorzystywać własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)
89. W przypadku wykrycia szkodliwego działania ransomware, moduł musi blokować aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.
90. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.
91. Administrator musi mieć możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.
92. Administrator musi posiadać możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.
93. Rozwiązanie musi być wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
94. Moduł musi posiadać możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.
95. Administrator musi posiadać możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
96. Musi istnieć możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.
97. Rozwiązanie musi potrafić automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
98. Rozwiązanie musi posiadać funkcjonalność kontroli uruchamianych aplikacji.
99. Tryb kontroli aplikacji musi umożliwiać uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji
100. Musi istnieć możliwość blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.
101. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.
102. Na wspieranych systemach Windows rozwiązanie musi pozwalać na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.

103. Administrator musi posiadać w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN
104. Rozwiązanie musi pozwalać na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD)
105. Administrator ma mieć możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.
106. Rozwiązanie musi pozwalać na wygenerowanie pliku za pomocą którego administrator może wywołać zdalne połączenie za pomocą usług Microsoft RDP (Remote Desktop).
107. Wygenerowany plik może być otwarty i wykorzystany do zdalnego połączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.

Centralna administracja

1. Portal zarządzający musi być dostępny w języku polskim.
2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi musi odbywać się w formie zaszyfrowanej.
3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które muszą łączyć się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.
4. Interfejs zarządzania musi posiadać funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamiania o zakończeniu licencji.
5. Interfejs musi być wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
6. Wykresy muszą być interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
7. Rozwiązanie musi posiadać dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
8. Musi istnieć możliwość eksportu listy wszystkich hostów do pliku CSV.
9. Administrator musi mieć możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego połączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
10. Administrator musi mieć możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.
11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
12. Rozwiązanie musi posiadać dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.
13. Musi istnieć możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.
14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego muszą zawierać liczbę i typ hostów, na których został wykryty brak danej poprawki.

15. Po wskazaniu danej poprawki administrator musi posiadać możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana.
16. Administrator ma mieć możliwość wglądu w historię instalowanych poprawek na chronionych hostach.
17. Rozwiązanie musi posiadać moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
19. Rozwiązanie musi posiadać wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
20. Administrator musi widzieć w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
21. Portal zarządzający musi umożliwiać dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.
22. Dodanie klucza licencyjnego musi skutkować aktywacją zawartości dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
23. Rozwiązanie musi mieć możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
24. Profile mogą być przypisane do pojedynczych hostów lub do grup.
25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.
26. W przypadku automatycznego przypisywania profili, system musi pozwalać na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.
27. Musi istnieć możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.
28. Rozwiązanie musi pozwalać administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.
29. Z poziomu portalu zarządzającego musi istnieć możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.
30. Pliki instalacyjne mają posiadać plików .EXE, .MSI .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.
31. Tworzone profile muszą dawać administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.
32. Administrator musi posiadać możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.
33. Administrator musi posiadać do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego.
34. Portal zarządzający musi pozwalać na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.
35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.
36. W ramach posiadanych licencji musi istnieć możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.

System EDR musi być zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zmusi być zapewniony przez przeglądarkę internetową.

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

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

Rozwiązanie musi posiadać możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:

- Microsoft Windows 10
- Microsoft Windows 11
- macOS 15 Sequoia
- macOS 14 Sonoma
- macOS 13 Ventura

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

- Microsoft® Windows Server 2016 Standard
- Microsoft® Windows Server 2016 Essentials
- Microsoft® Windows Server 2016 Datacenter
- Microsoft® Windows Server 2016 Core
- Microsoft® Windows Server 2019 Standard
- Microsoft® Windows Server 2019 Essentials
- Microsoft® Windows Server 2019 Datacenter
- Microsoft® Windows Server 2019 Core
- Microsoft® Windows Server 2022 Standard
- Microsoft® Windows Server 2022 Essentials
- Microsoft® Windows Server 2022 Datacenter
- Microsoft® Windows Server 2022 Core

Wspierane przeglądarki internetowe:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

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

1. Oprogramowanie instalowane na stacjach końcowych i serwerach, zwane dalej agentem, ma mieć możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.

2. Agent instalowany na stacjach końcowych i serwerach musi posiadać możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.
3. Agent instalowany na stacjach końcowych i serwerach musi posiadać możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.
4. Oprogramowanie ma nie wymagać restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach.
5. Dane zebrane przez agenta instalowanego na stacjach końcowych muszą być przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.
6. Agent instalowany na stacjach końcowych i serwerach musi monitorować i zbierać informacje na temat co najmniej następujących zdarzeń:
 - dostęp do pliku;
 - tworzenie nowego procesu;
 - nawiązane połączenia sieciowe;
 - wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
 - zawartość skryptów uruchamianych na monitorowanej stacji.
7. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń muszą odbywać się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.
8. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, muszą być kompresowane w celu optymalizacji wykorzystania łącza sieciowych.
9. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, musi odbywać się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
10. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, musi wspierać komunikację za pomocą serwera pośredniczącego http (http proxy).
11. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej muszą być buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.
12. Dane zbierane przez agentów na stacjach końcowych i serwerach muszą być przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.
14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym.
16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
17. Rozwiązanie musi posiadać możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
18. Każda detekcja musi zawierać co najmniej następujące informacje:
 - Listę urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
 - Data i czas wystąpienia podejrzanych zdarzeń.
 - Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.

- Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
 - Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
 - Poziom ryzyka, określający istotność danej detekcji.
 - Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).
19. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, muszą zawierać odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).
 20. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, muszą zawierać odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).
 21. Rozwiązanie musi umożliwiać oznaczanie wygenerowanych detekcji jako błędne.
 22. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
 23. Rozwiązanie musi posiadać możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
 24. Rozwiązanie musi pozwalać na dodanie własnego komentarza przy wykrytej detekcji.
 25. Rozwiązanie musi umożliwiać wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
 26. Rozwiązanie musi pozwalać na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
 27. Rozwiązanie musi pozwalać na izolację sieciową komputerów przez administratora.
 28. Rozwiązanie musi umożliwiać tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
 29. Rozwiązanie musi umożliwiać wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.
 30. Rozwiązanie musi umożliwiać tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
 31. Rozwiązanie musi pozwalać na eksport raportów, w postaci plików PDF.
 32. Rozwiązanie musi wspierać dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
 33. Konsola centralnego zarządzania musi oferować interfejs w języku Polskim.
 34. Konsola zarządzająca musi być wyposażona w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
 35. Rozwiązanie musi umożliwiać wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.
 36. Konsola musi być wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
 37. Lista urządzeń posiadających zainstalowanego agenta systemu EDR musi zawierać informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.

38. Administrator musi widzieć w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
39. Portal zarządzający musi umożliwiać dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EPP, mechanizmów zarządzania podatnościami.
40. Dodanie klucza licencyjnego musi skutkować aktywowaniem zawartości zakładki obsługującej dany produkt w portalu zarządzającym.

Usługa MDR musi być udostępniana jako rozszerzenie dla istniejącej infrastruktury klienta obejmująca system ochrony antywirusowej i system EDR. Usługa zapewnia ciągły monitoring 24/7 środowiska elementów i oraz reagowanie na detekcje zgodnie z ustalonymi wcześniej z klientem uprawnieniami. Usługa reakcji MDR musi obejmować minimum jedno urządzenie w okresie trwania usługi, z możliwością rozszerzenia usługi w trakcie jej trwania.

1. Usługa musi zapewniać stałe monitorowanie środowiska usługobiorcy.
2. Konsola do komunikacji i zarządzania środowiskiem musi posiadać polski interfejs użytkownika.
3. Rozwiązanie na bazie zebranych danych musi generować detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agenta ze stacji roboczych i serwerów.
4. W ramach usługi certyfikowani analitycy producenta muszą identyfikować potencjalne incydenty bezpieczeństwa poprzez walidację i badanie detekcji w celu ustalenia, czy incydent wymaga wykonania dalszych działań naprawczych.
5. Detekcje muszą być kategoryzowane przez analityków producenta oprogramowania na minimum następujące statusy:
 - Fałszywie pozytywne
 - Podejrzana aktywność
 - Potwierdzone zagrożenie
6. Detekcje w momencie jej potwierdzenia jako rzeczywiste zagrożenie powinny być odpowiednio eskalowane przez analityków producenta.
7. Analitycy producenta jeśli zostali do tego upoważnieni muszą wykonać działania ograniczające rozprzestrzenianie się zagrożenia, działania zaradcze i działania mające na celu przywrócić normalne działanie.
8. Analitycy producenta muszą powiadomić osoby wyznaczoną do kontaktu w momencie wykrycia rzeczywistego incydentu.
9. Komunikacja z analitykami producenta musi być dostępna podczas zdarzenia w sekcji komentarzy dla wykrytej detekcji, lub poprzez rozmowę telefoniczną.
10. Usługa posiada możliwość dokupienia specjalnej usługi polegającej na przyznaniu większej ilości zasobów reagowania na incydenty objętych umową SLA, w przypadku wykrycia detekcji o większym zagrożeniu dla środowiska usługobiorcy.
11. Rozwiązanie musi posiadać akredytację rządową uzyskaną przez UK National Cyber Security Centre i Federal Office for Information Security.
12. Analitycy w momencie niwelacji detekcji przekazują sugestie dotyczące dalszych kroków mających na celu zapobiegnięcie powrotu incydentu w przyszłości.

- dostawa serwerów plików NAS wraz dyskami dla Urzędu Miasta i Gminy w Pieszcach oraz Jednostek Podległych

Przedmiotem niniejszego zamówienia jest dostawa 8 (ośmiu) sztuk fabrycznie nowych, wolnych od wad fizycznych i prawnych serwerów plików NAS.

Wszystkie oferowane urządzenia muszą być nieużywane, nierafabrykowane, a także nie mogły być przedmiotem ekspozycji, testów ani pokazów. Urządzenia muszą spełniać wszystkie parametry techniczne i wymagania określone w niniejszym dokumencie.

Procesor	Procesor 64 bit x86 o takowaniu nie mniejszym niż 2.2 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 8GB
Pamięć RAM liczba slotów	Minimum 2 sloty
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 64GB
Pamięć Flash	Nie mniej niż 5 GB
Liczba zatok na dyski	Minimum 4 zatoki 3,5"
Obsługiwane dyski	3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" SATA SSD
Dyski	Wymagane są 4 dyski każdy o pojemności 6 TB, z interfejsem SATA 6 Gb/s, prędkością 7200 RPM, 256 MB pamięci cache, technologią CMR, MTBF (średni czas bezawaryjnej pracy): 2 miliony godzin, Zaprojektowane do pracy 24/7 w środowiskach NAS.
Wbudowane w urządzenie interfejsy na dyski M2	Wymagane min. 2 x M2 PCIe Gen3x1
Możliwość stosowania dysków twardych o pojemności	do 32TB
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Minimum 2 RJ-45
Diody LED	Minimum Status, LAN, HDD
Porty USB 3.2 Gen2	Minimum 3
Port PCIe	Tak, minimum 2 Gen3x4
Przyciski	Reset, Zasilanie
Typ obudowy	Tower
Dopuszczalna temperatura pracy	od 0 do 40°C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Max. 250 W
Specyfikacja oprogramowania	
Obsługa dwóch systemów operacyjnych	Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS

Wymagania dla systemu operacyjnego opartego o system plików EXT4	
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android

Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker

Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja	3 lata

- dostawa zasilaczy awaryjnych UPS typu rack dla Urzędu Miasta i Gminy w Pieszcach oraz Jednostek Podległych

- dostawa zasilaczy awaryjnych UPS typu rack – TYP 1:

Przedmiotem niniejszego zamówienia jest dostawa 8 (ośmiu) sztuk fabrycznie nowych, wolnych od wad fizycznych i prawnych zasilaczy awaryjnych UPS.

Każde z oferowanych urządzeń musi spełniać minimalne parametry techniczne określone w poniższej tabeli.

Nazwa komponentu	Wymagane parametry techniczne
Technologia	online, VFI-SS-111,
Moc wyjściowa	3kVA/3kW; PF=1
Obudowa	Rack/Tower (wraz z UPS dostarczyć zestaw do montażu w szafie rack)
Napięcie wejściowe	110 ÷ 300 V AC ± 2 %
Napięcie znamionowe (wartość skuteczna)	230V AC
Prąd znamionowy (wejście)	15,6A
Częstotliwość napięcia wejściowego (zakres oraz tolerancja)	45 ÷ 55 / 55 ÷ 65 Hz ± 1 Hz
Częstotliwość znamionowa napięcia wejściowego	50Hz / 60Hz
Zniekształcenia prądu wejściowego THDi	< 5%
Zakres napięcia wyjściowego	200/208/220/230/240V AC konfigurowalne z poziomu oprogramowania oraz z menu zasilacza na wyświetlaczu LCD (domyślnie 230V AC

Zniekształcenia napięcia wyjściowego THDu	< 1% dla Pmax (liniowe) < 5% (nieliniowe wg PN EN 62040-3)
Gniazda wyjściowe	4x IEC320 C13 (10A) sterowalne + 4x IEC320 C13 (10A) + 1x IEC320 C19 (16A)
Akumulatory wewnętrzne UPS	Minimum 6szt akumulatorów 12V9Ah
Moduły bateryjne	Opcja – możliwość podpięcia do 4szt modułów (każdy z minimum 12szt akumulatorów 12V9Ah)
Czas podtrzymania UPS dla obciążenia 3kW/2,4kW/1,5kW	3,5 / 5 / 10 min
Czas podtrzymania UPS + MODUŁ dla obciążenia 3kW/2,4kW/1,5kW	17 / 23 / 40 min
Przeciążalność	105-125% - 5min / 125-150% - 30s / >150% - 500ms
EPO	Wymagane – standard NC
Sygnalizacja	akustyczno-diodowa, wyświetlacz LCD oraz diody sygnalizujące usterkę, pracę baterijną, pracę w trybie online, obejście bypass
Język oprogramowania	polski i angielski do wyboru z poziomu interfejsu użytkownika
Wymagane certyfikaty	CE, ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu; (załączyć dokument)
Komunikacja z urządzeniem	RS232, USB HID, styki bezpotencjałowe 1-wejście; 1-wyjście; SNMP – wymagane - dopuszczalne jako opcjonalna karta
Wymiary UPS (rack) (wys x szer x gł)	Nie więcej niż 86 x 439 x 600 mm
Oprogramowanie do monitorowania pracy zasilacza UPS	Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów (potwierdzone oświadczeniem producenta oprogramowania)
Możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPS'ów w oprogramowaniu	Wymagane

Konfiguracja minimalnego poziomu naładowania baterii. UPS po rozładowaniu baterii przed samoczynnym załączeniem zasilania wyjść (po powrocie zasilania sieciowego) będzie musiał naładować baterie do tego poziomu. załączenie zasilania wyjść może nastąpić tylko wtedy, gdy UPS zgromadzi niezbędny zapas energii na wypadek kolejnego zaniku.	Wymagane
Oprogramowanie - funkcjonalność	Funkcja umożliwiająca załączenie urządzeń o zwiększonym prądzie rozruchowym bez przeciążania falownika UPS Uruchom poprzez Bypass - UPS zawsze przed załączeniem zasilania wyjść na kilka sekund powinno załączyć się zasilanie poprzez Bypass i przełączyć w zasilanie wyjść poprzez falownik (normalny tryb pracy).
Serwis producenta	wymagany, zlokalizowany na terenie Polski, autoryzacja serwisowa lub oświadczenie producenta - załączyć do oferty
Gwarancja	Minimum 24 miesiące elektronika, 24 miesiące akumulatory, serwis door to door, czas naprawy 5 dni roboczych
Dokumentacja	Instrukcja w języku polskim

- dostawa zasilaczy awaryjnych UPS typu rack – TYP 2:

Przedmiotem niniejszego zamówienia jest dostawa 30 (trzydziestu) sztuk fabrycznie nowych, wolnych od wad fizycznych i prawnych zasilaczy awaryjnych UPS.

Każde z oferowanych urządzeń musi spełniać minimalne parametry techniczne określone w poniższej tabeli.

Nazwa komponentu	Wymagane parametry techniczne
Technologia	Line-interactive (VI)
Moc wyjściowa	2200VA/1200W
Obudowa	Tower
Napięcie wejściowe – zakres	170 ÷ 280 V AC ± 7 %
Częstotliwość wejściowa – zakres	45 – 55 Hz ± 1 Hz
Napięcie wyjściowe – zakres	230 V AC ± 10%
Progi przełączania: UPS - sieć	176 V ÷ 274 V AC ± 7 %
Akumulatory wewnętrzne	2x 12V / 9Ah VRLA
Czas podtrzymania dla 50% Pmax [600W]	Nie mniej niż 6 minut

Maksymalny czas ładowania baterii wewnętrznych UPS - po 80% wyładowaniu baterii	6h
Przylącze zasilania UPS	IEC320 C14
Przylącza wyjściowe (liczba i typ gniazd)	2 x PN-E-93201 2 x IEC 320 C13 (10 A)
Interfejs komunikacyjny	USB HID
Sygnalizacja optyczna	Wyświetlacz LCD
Filtr teleinformatyczny (linii danych) – RJ45	LAN 10/100 Base-T
Oprogramowanie do monitorowania pracy zasilacza UPS	Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności; możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów (potwierdzone oświadczeniem producenta oprogramowania); oświadczenie producenta o posiadaniu pełnych praw oraz licencji do oprogramowania
Serwis producenta	wymagany, zlokalizowany na terenie Polski, autoryzacja serwisowa lub oświadczenie producenta - załączyć do oferty
Gwarancja	Minimum 24 miesiące elektronika, 12 miesięcy akumulatory, serwis door to door, czas naprawy 14 dni roboczych
Dokumentacja	Instrukcja w języku polskim; oświadczenie producenta o posiadaniu licencji oraz pełnych praw do oprogramowania do monitorowania pracy UPS

- dostawa routerów brzegowych dla Urzędu Miasta i Gminy w Pieszcach oraz Jednostek Podległych

a) Dostawa urządzenie typu UTM dla Urzędu Miasta i Gminy w Pieszcach

Przedmiotem niniejszego zamówienia jest dostawa 1 (jednego) sztuk fabrycznie nowych urządzeń typu firewall/router klasy UTM.

Wszystkie oferowane urządzenia muszą być fabrycznie nowe, nieużywane, nierafabrykowane, wolne od wad fizycznych i prawnych oraz pochodzić z oficjalnego polskiego kanału dystrybucji. Urządzenia nie mogły być przedmiotem ekspozycji, testów ani pokazów.

Lp.	Nazwa parametru	Wymagane parametry
1	Obudowa	Obudowa urządzenia musi być pozbawiona wentylatora oraz przystosowana do montażu w standardowej szafie 19" (w zestawie muszą znajdować się odpowiednie uchwyty). Obudowa urządzenia nie może być wyższa niż 1U.
2	Zasilanie	Maksymalna moc pobierana przez urządzenie nie może przekraczać 22W.
3	Elementy mechaniczne	Urządzenie nie może posiadać wbudowanego dysku/dysków twardych.

4	Interfejsy	Minimum 6 konfigurowalnych portów 100M/1G Ethernet (RJ-45), minimum 2 konfigurowalne porty 100M/1G/2.5G Ethernet (RJ-45), port konsoli (RJ45), port USB 3.0 Type-A. Urządzenie musi wspierać funkcjonalność Link Aggregation (LAG). Urządzenie musi wspierać funkcjonalność WAN load balancing.
5	Tryby pracy	Urządzenie musi umożliwiać zdalną konfigurację i monitorowanie poprzez panel sterowania dostępny w technologii chmury, dostarczony bezpłatnie przez producenta urządzenia
6	VLAN 802.1q	Urządzenie musi umożliwiać kreowanie interfejsów VLAN 802.1q. Funkcjonalność ta musi być dostępna w standardzie (bez konieczności zakupu dodatkowych licencji/modułów) Urządzenie powinno obsługiwać nie mniej niż 32 interfejsów VLAN
7	Anti-Malware	Urządzenie musi pozwalać na aktywację rocznej licencji funkcjonalności Anti-Malware w cenie urządzenia
8	IPS (IDP)	Urządzenie musi pozwalać na aktywację rocznej licencji funkcjonalności IPS (IDP) w cenie urządzenia
9	Application Patrol	Urządzenie musi pozwalać na aktywację rocznej licencji funkcjonalności Application Patrol w cenie urządzenia
10	Web filtering	Urządzenie musi pozwalać na aktywację rocznej licencji funkcjonalności Web filtering w cenie urządzenia
11	Reputation Filter	Urządzenie musi pozwalać na aktywację rocznej licencji funkcjonalności Reputation Filter w cenie urządzenia
12	Sandboxing	Urządzenie musi pozwalać na aktywację rocznej licencji funkcjonalności Sandboxing w cenie urządzenia
13	Security Profile Sync	Urządzenie musi pozwalać na aktywację rocznej licencji funkcjonalności Security Profile Sync w cenie urządzenia
14	Device Insight	Urządzenie musi pozwalać na aktywację rocznej licencji funkcjonalności Device Insight w cenie urządzenia
15	SSL (HTTPS) inspection	Urządzenie musi pozwalać na aktywację funkcji SSL (HTTPS) inspection
16	2-Factor Authentication	Urządzenie musi pozwalać na aktywację funkcji 2-Factor Authentication
17	Wysoka dostępność	Urządzenie musi umożliwiać połączenie dwóch bram w trybie HA.
18	VPN	Obsługa 100 równoczesnych połączeń IPSec VPN. Obsługa IKEv2/IPSec, Tailscale Obsługa funkcji Auto-link VPN Obsługa funkcji Manual-link VPN Obsługa funkcji VPN Topology Przepustowość VPN nie powinna być mniejsza niż 1200 Mbps
19	Kontroler WLAN	Urządzenie musi posiadać wbudowany kontroler WLAN umożliwiający zarządzanie do 40 punktami dostępowymi.
20	Monitorowanie oraz raportowanie zdarzeń	W cenie urządzenia powinna być uwzględniona roczna licencja na aplikację chmurową przeznaczoną do analizowania logów i generowania raportów dotyczących funkcjonowania bramy.
21	Wydajność	Przepustowość dla firewall'a nie powinna być mniejsza niż 6 500 Mbps Przepustowość UTM (aktywowane moduły AV, IDP) nie powinna być mniejsza niż 1 800 Mbps
22	Maksymalna liczba	Maksymalna liczba równoległe obsługiwanych sesji TCP nie może być mniejsza niż 600 000

	równoczesnych sesji	
23	Rozpraszanie ciepła (BTU/hr)	Parametr ten nie powinien być wyższy niż 58.75
24	Gwarancja	Minimum 5 lat gwarancji na oferowane urządzenie
25	Serwis	W przypadku awarii urządzenia, wysyłka zastępczego produktu następuje w następnym dniu roboczym, po którym zgłoszona zostanie awaria. Urządzenie powinno być objęte w/w opcją serwisową w okresie nie krótszym niż 5 lat.
26	Wymagane Certyfikaty	Bezpieczeństwo <ul style="list-style-type: none"> • LVD (EN62368-1) • BSMI EMC <ul style="list-style-type: none"> • FCC Part 15 (Class B) • CE EMC (Class B) • RCM (Class B) • BSMI
27	Inne	Urządzenie musi być fabrycznie nowe i pochodzić z polskiego kanału dystrybucji

b) Dostawa routerów dla jednostek podległych

Przedmiotem niniejszego zamówienia jest dostawa 4 (czterech) sztuk fabrycznie nowych urządzeń typu firewall/router klasy UTM.

Wszystkie oferowane urządzenia muszą być fabrycznie nowe, nieużywane, nierafabrykowane, wolne od wad fizycznych i prawnych oraz pochodzić z oficjalnego polskiego kanału dystrybucji. Urządzenia nie mogły być przedmiotem ekspozycji, testów ani pokazów.

Lp.	Nazwa parametru	Wymagane parametry
1	Obudowa	Obudowa urządzenia musi być pozbawiona wentylatora.
2	Zasilanie	Maksymalna moc pobierana przez urządzenie nie może przekraczać 9W.
3	Elementy mechaniczne	Urządzenie nie może posiadać wbudowanego dysku/dysków twardych.
4	Interfejsy	Minimum 5 konfigurowalnych portów 100M/1G Ethernet (RJ-45), port konsoli (Rj45), port USB 3.0 Type-A, Urządzenie musi wspierać funkcjonalność Link Aggregation (LAG), Urządzenie musi wspierać funkcjonalność WAN load balancing.
5	Tryby pracy	Urządzenie musi umożliwiać zdalną konfigurację i monitorowanie poprzez panel sterowania dostępny w technologii chmury, dostarczony bezpłatnie przez producenta urządzenia
6	VLAN 802.1q	Urządzenie musi umożliwiać kreowanie interfejsów VLAN 802.1q. Funkcjonalność ta musi być dostępna w standardzie (bez konieczności zakupu dodatkowych licencji/modułów) Urządzenie powinno obsługiwać nie mniej niż 8 interfejsów VLAN
7	Anti-Malware	Urządzenie może pozwalać na aktywację licencji funkcjonalności Anti-Malware
8	IPS (IDP)	Urządzenie może pozwalać na aktywację licencji funkcjonalności IPS (IDP)

9	Application Patrol	Urządzenie może pozwalać na aktywację licencji funkcjonalności Application Patrol
10	Web filtering	Urządzenie może pozwalać na aktywację licencji funkcjonalności Web filtering
11	Reputation Filter	Urządzenie może pozwalać na aktywację licencji funkcjonalności Reputation Filter
12	Sandboxing	Urządzenie może pozwalać na aktywację licencji funkcjonalności Sandboxing
13	Security Profile Sync	Urządzenie może pozwalać na aktywację licencji funkcjonalności Security Profile Sync
14	Device Insight	Urządzenie musi pozwalać na aktywację licencji funkcjonalności Device Insight
15	SSL (HTTPS) inspection	Urządzenie musi pozwalać na aktywację funkcji SSL (HTTPS) inspection
16	2-Factor Authentication	Urządzenie musi pozwalać na aktywację funkcji 2-Factor Authentication
17	VPN	Obsługa 20 równoczesnych połączeń IPsec VPN. Obsługa IKEv2/IPsec, Tailscale Obsługa funkcji Auto-link VPN Obsługa funkcji Manual-link VPN Obsługa funkcji VPN Topology Przepustowość VPN nie powinna być mniejsza niż 500 Mbps
18	Kontroler WLAN	Urządzenie musi posiadać wbudowany kontroler WLAN umożliwiający zarządzanie do 12 punktami dostępowymi.
19	Monitorowanie oraz raportowanie zdarzeń	W cenie urządzenia powinna być uwzględniona roczna licencja na aplikację chmurową przeznaczoną do analizowania logów i generowania raportów dotyczących funkcjonowania bramy.
20	Wydajność	Przepustowość dla firewall'a nie powinna być mniejsza niż 2000 Mbps Przepustowość UTM (aktywowane moduły AV, IDP) nie powinna być mniejsza niż 600 Mbps
21	Maksymalna liczba równoczesnych sesji	Maksymalna liczba równocześnie obsługiwanych sesji TCP nie może być mniejsza niż 100 000
22	Rozpraszanie ciepła (BTU/hr)	Parametr ten nie powinien być wyższy niż 32.42
23	Gwarancja	Minimum 5 lat gwarancji na oferowane urządzenie
24	Serwis	W przypadku awarii urządzenia, wysyłka zastępczego produktu następuje w następnym dniu roboczym, po którym zgłoszona zostanie awaria. Urządzenie powinno być objęte w/w opcją serwisową w okresie nie krótszym niż 5 lat.
25	Wymagane Certyfikaty	Bezpieczeństwo • LVD (EN62368-1) • BSMI EMC • FCC Part 15 (Class B) • CE EMC (Class B) • RCM (Class B) • BSMI
26	Inne	Urządzenie musi być fabrycznie nowe i pochodzić z polskiego kanału dystrybucji

- dostawa oprogramowania do wykonywania kopii zapasowych dla Urzędu Miasta i Gminy w Pieszycach oraz Jednostek Podległych

Zamawiający wymaga dostawy oprogramowania do wykonywania kopii zapasowych spełniającego następujące wymagania dla konkretnych Jednostek jak poniżej.

Zamawiający wymaga dostarczenia oprogramowania do tworzenia kopii zapasowych dla Urzędu oraz jednostek podległych. Oprogramowanie musi być objęte licencją wieczystą i zawierać standardowe wsparcie techniczne świadczone przez okres 12 miesięcy.

Urząd Miasta i Gminy w Pieszycach

I	Wymagania minimalne
1	Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji
a	Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012
b	Vmware vSphere min. w wersjach v5.5 - 9.0
c	Nutanix AHV v6.5, v6.10
d	Maszyny fizyczne: Windows Server 2025, 2022, 2019, 2016, 2012R2, 2012
e	Microsoft 365 (Exchange online, One Drive for Business, Sharepoint)
f	Proxmox Virtual Environment min. w wersji 8.0
2	Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V
3	Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:
a	na serwerze Windows lub Linux
b	jako maszyna wirtualna VMware
c	jako maszyna wirtualna Amazon
d	na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital
4	Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS
5	Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania
6.	Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
II	Licencjonowanie
1	Oprogramowanie powinno być licencjonowane per maszyna wirtualna (w przypadku środowisk wirtualnych jak Hyper-V, VMware, Proxmox, AWS EC2) lub per maszyna fizyczna w przypadku fizycznych serwerów. Licencjonowanie powinno być realizowane w wariancie subskrypcji, w którym licencja ma określony termin ważności.
2	Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 50 chronionych zasobów jak maszyny wirtualne lub maszyny fizyczne.
3	W ramach dostawy wymagane jest dostarczenie licencji na ochronę 3 maszyn fizycznych z systemem operacyjnym Windows Server lub Linux (w wersji serwerowej)

4	W ramach dostawy wymagane jest dostarczenie licencji na ochronę 40 maszyn fizycznych z systemem operacyjnym Windows 10 Pro lub Ubuntu Desktop
5	Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska
III	Ochrona danych
1	Oprogramowanie musi posiadać funkcje backupu i replikacji:
a	Backup maszyn wirtualnych Vmware
b	Replikacja maszyn wirtualnych Vmware (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
c	Backup maszyn wirtualnych Hyper-V
d	Replikacja maszyn wirtualnych Hyper-V (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
e	Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
f	Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
g	Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
h	Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
i	Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych. Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem
j	Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
k	Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
l	Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach
IV	Optymalizacja wykorzystania miejsca na dane
1	Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
a	Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
b	Kompresja backupu, w tym konfigurowalny stopień kompresji
c	Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne
V	Spójność danych
1	Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
a	Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
b	Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
c	Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji:
	Microsoft Exchange 2013, 2016, 2019
	Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022

d	Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
e	Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
f	Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
g	Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji
VI	Przywracanie danych
l	Oprogramowanie musi posiadać poniższe funkcje:
a	Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
b	Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)
c	Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
d	Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
	Microsoft Exchange
	MS Active Directory
	MS SQL
e	Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.
VI	I Wydajność
l	Oprogramowanie do backupu musi pozwalać na:
a	Tworzenie backupu i replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
b	Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
c	Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN
d	Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
e	Wsparcie dla urządzeń oferujących dodatkową deduplikację danych
VI	II Zarządzanie
l	Oprogramowanie musi pozwalać na następujące formy zarządzania:
a	Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
b	Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
c	Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania
d	Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.
e	Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
f	Oprogramowanie musi umożliwiać integrację z Active Directory

g	Oprogramowanie musi wspierać tzw. tryb multi tenant, umożliwiający podzielenie oprogramowania do backupu na kilka podinstancji zarządzanych z odrębnych interfejsów w celu rozłożenia zarządzania w złożonych środowiskach
---	--

Zakład Gospodarki Mieszkaniowej w Pieszcach

I	Wymagania minimalne
1	Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji
a	Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012
b	Vmware vSphere min. w wersjach v5.5 - 9.0
c	Nutanix AHV v6.5, v6.10
d	Maszyny fizyczne: Windows Server 2025, 2022, 2019, 2016, 2012R2, 2012
e	Microsoft 365 (Exchange online, One Drive for Business, Sharepoint)
f	Proxmox Virtual Environment min. w wersji 8.0
2	Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V
3	Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:
a	na serwerze Windows lub Linux
b	jako maszyna wirtualna VMware
c	jako maszyna wirtualna Amazon
d	na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital
4	Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS
5	Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania
6.	Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
II	Licencjonowanie
1	Oprogramowanie powinno być licencjonowane per maszyna wirtualna (w przypadku środowisk wirtualnych jak Hyper-V, VMware, Proxmox, AWS EC2) lub per maszyna fizyczna w przypadku fizycznych serwerów. Licencjonowanie powinno być realizowane w wariancie subskrypcji, w którym licencja ma określony termin ważności.
2	Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 50 chronionych zasobów jak maszyny wirtualne lub maszyny fizyczne.
3	W ramach dostawy wymagane jest dostarczenie licencji na ochronę 1 maszyn fizycznych z systemem operacyjnym Windows Server lub Linux (w wersji serwerowej)
4	W ramach dostawy wymagane jest dostarczenie licencji na ochronę 7 maszyn fizycznych z systemem operacyjnym Windows 10 Pro lub Ubuntu Desktop
5	Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska
III	Ochrona danych
1	Oprogramowanie musi posiadać funkcje backupu i replikacji:

a	Backup maszyn wirtualnych Vmware
b	Replikacja maszyn wirtualnych Vmware (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
c	Backup maszyn wirtualnych Hyper-V
d	Replikacja maszyn wirtualnych Hyper-V (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
e	Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
f	Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
g	Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
h	Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
i	Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych. Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem
j	Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
k	Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
l	Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach
IV	Optymalizacja wykorzystania miejsca na dane
l	Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
a	Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
b	Kompresja backupu, w tym konfigurowalny stopień kompresji
c	Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne
V	Spójność danych
l	Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
a	Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
b	Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
c	Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji:
	Microsoft Exchange 2013, 2016, 2019
	Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022
d	Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
e	Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
f	Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania

g	Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji
VI	Przywracanie danych
l	Oprogramowanie musi posiadać poniższe funkcje:
a	Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
b	Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)
c	Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
d	Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
	Microsoft Exchange
	MS Active Directory
	MS SQL
e	Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji VMware i Hyper-V i odwrotnie.
VI	
I	Wydajność
l	Oprogramowanie do backupu musi pozwalać na:
a	Tworzenie backupu i replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
b	Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
c	Backup z pominięciem sieci LAN dzięki opcjom dostępu bezpośredniego w sieciach SAN
d	Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
e	Wsparcie dla urządzeń oferujących dodatkową deduplikację danych
VI	
II	Zarządzanie
l	Oprogramowanie musi pozwalać na następujące formy zarządzania:
a	Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
b	Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
c	Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania
d	Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.
e	Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
f	Oprogramowanie musi umożliwiać integrację z Active Directory
g	Oprogramowanie musi wspierać tzw. tryb multi tenant, umożliwiający podzielenie oprogramowania do backupu na kilka podinstancji zarządzanych z odrębnych interfejsów w celu rozłożenia zarządzania w złożonych środowiskach

Centrum Usług Społecznych w Pieszcach

I	Wymagania minimalne
1	Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji
a	Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012
b	Vmware vSphere min. w wersjach v5.5 - 9.0
c	Nutanix AHV v6.5, v6.10
d	Maszyny fizyczne: Windows Server 2025, 2022, 2019, 2016, 2012R2, 2012
e	Microsoft 365 (Exchange online, One Drive for Business, Sharepoint)
f	Proxmox Virtual Environment min. w wersji 8.0
2	Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V
3	Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:
a	na serwerze Windows lub Linux
b	jako maszyna wirtualna VMware
c	jako maszyna wirtualna Amazon
d	na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital
4	Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS
5	Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania
6.	Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
II	Licencjonowanie
1	Oprogramowanie powinno być licencjonowane per maszyna wirtualna (w przypadku środowisk wirtualnych jak Hyper-V, VMware, Proxmox, AWS EC2) lub per maszyna fizyczna w przypadku fizycznych serwerów. Licencjonowanie powinno być realizowane w wariancie subskrypcji, w którym licencja ma określony termin ważności.
2	Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 50 chronionych zasobów jak maszyny wirtualne lub maszyny fizyczne.
4	W ramach dostawy wymagane jest dostarczenie licencji na ochronę 15 maszyn fizycznych z systemem operacyjnym Windows 10 Pro lub Ubuntu Desktop
5	Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska
III	Ochrona danych
1	Oprogramowanie musi posiadać funkcje backupu i replikacji:
a	Backup maszyn wirtualnych VMware
b	Replikacja maszyn wirtualnych VMware (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
c	Backup maszyn wirtualnych Hyper-V
d	Replikacja maszyn wirtualnych Hyper-V (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
e	Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych

f	Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
g	Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
h	Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
i	Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem
j	Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
k	Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
l	Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach
IV	Optymalizacja wykorzystania miejsca na dane
l	Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
a	Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
b	Kompresja backupu, w tym konfigurowalny stopień kompresji
c	Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne
V	Spójność danych
l	Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
a	Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
b	Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
c	Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji:
	Microsoft Exchange 2013, 2016, 2019
	Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022
d	Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
e	Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
f	Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
g	Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji
VI	Przywracanie danych
l	Oprogramowanie musi posiadać poniższe funkcje:
a	Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
b	Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)

c	Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
d	Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
	Microsoft Exchange
	MS Active Directory
	MS SQL
e	Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.
VI	
I	Wydajność
1	Oprogramowanie do backupu musi pozwalać na:
a	Tworzenie backupu i replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
b	Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
c	Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN
d	Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
e	Wsparcie dla urządzeń oferujących dodatkową deduplikację danych
VI	
II	Zarządzanie
1	Oprogramowanie musi pozwalać na następujące formy zarządzania:
a	Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
b	Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
c	Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania
d	Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.
e	Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
f	Oprogramowanie musi umożliwiać integrację z Active Directory
g	Oprogramowanie musi wspierać tzw. tryb multi tenant, umożliwiający podzielenie oprogramowania do backupu na kilka podinstancji zarządzanych z odrębnych interfejsów w celu rozłożenia zarządzania w złożonych środowiskach

Szkoła Podstawowa nr 1 w Pieszcach im. Pieszyckiej Harcerskiej Organizacji Podziemnej

I	Wymagania minimalne
1	Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji
a	Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012
b	Vmware vSphere min. w wersjach v5.5 - 9.0
c	Nutanix AHV v6.5, v6.10

d	Maszyny fizyczne: Windows Server 2025, 2022, 2019, 2016, 2012R2, 2012
e	Microsoft 365 (Exchange online, One Drive for Business, Sharepoint)
f	Proxmox Virtual Environment min. w wersji 8.0
2	Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V
3	Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:
a	na serwerze Windows lub Linux
b	jako maszyna wirtualna VMware
c	jako maszyna wirtualna Amazon
d	na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital
4	Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS
5	Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania
6.	Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
II	Licencjonowanie
1	Oprogramowanie powinno być licencjonowane per maszyna wirtualna (w przypadku środowisk wirtualnych jak Hyper-V, VMware, Proxmox, AWS EC2) lub per maszyna fizyczna w przypadku fizycznych serwerów. Licencjonowanie powinno być realizowane w wariancie subskrypcji, w którym licencja ma określony termin ważności.
2	Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 50 chronionych zasobów jak maszyny wirtualne lub maszyny fizyczne.
4	W ramach dostawy wymagane jest dostarczenie licencji na ochronę 5 maszyn fizycznych z systemem operacyjnym Windows 10 Pro lub Ubuntu Desktop
5	Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska
III	Ochrona danych
1	Oprogramowanie musi posiadać funkcje backupu i replikacji:
a	Backup maszyn wirtualnych VMware
b	Replikacja maszyn wirtualnych VMware (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
c	Backup maszyn wirtualnych Hyper-V
d	Replikacja maszyn wirtualnych Hyper-V (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
e	Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
f	Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
g	Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
h	Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
i	Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem

j	Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
k	Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
l	Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach
IV	Optymalizacja wykorzystania miejsca na dane
l	Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
a	Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
b	Kompresja backupu, w tym konfigurowalny stopień kompresji
c	Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne
V	Spójność danych
l	Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
a	Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
b	Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
c	Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji:
	Microsoft Exchange 2013, 2016, 2019
	Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022
d	Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
e	Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
f	Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
g	Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji
VI	Przywracanie danych
l	Oprogramowanie musi posiadać poniższe funkcje:
a	Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
b	Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)
c	Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
d	Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
	Microsoft Exchange
	MS Active Directory
	MS SQL
e	Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.

VI	
I	Wydajność
1	Oprogramowanie do backupu musi pozwalać na:
a	Tworzenie backupu i replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
b	Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
c	Backup z pominięciem sieci LAN dzięki opcjom dostępu bezpośredniego w sieciach SAN
d	Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
e	Wsparcie dla urządzeń oferujących dodatkową deduplikację danych
VI	
II	Zarządzanie
1	Oprogramowanie musi pozwalać na następujące formy zarządzania:
a	Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
b	Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
c	Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania
d	Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.
e	Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
f	Oprogramowanie musi umożliwiać integrację z Active Directory
g	Oprogramowanie musi wspierać tzw. tryb multi tenant, umożliwiający podzielenie oprogramowania do backupu na kilka podinstancji zarządzanych z odrębnymi interfejsów w celu rozłożenia zarządzania w złożonych środowiskach

Przedszkole Publiczne nr 2 w Pieszcach

I	Wymagania minimalne
1	Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji
a	Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012
b	Vmware vSphere min. w wersjach v5.5 - 9.0
c	Nutanix AHV v6.5, v6.10
d	Maszyny fizyczne: Windows Server 2025, 2022, 2019, 2016, 2012R2, 2012
e	Microsoft 365 (Exchange online, One Drive for Business, Sharepoint)
f	Proxmox Virtual Environment min. w wersji 8.0
2	Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V
3	Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:
a	na serwerze Windows lub Linux
b	jako maszyna wirtualna VMware
c	jako maszyna wirtualna Amazon

d	na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital
4	Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS
5	Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania
6.	Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
II	Licencjonowanie
1	Oprogramowanie powinno być licencjonowane per maszyna wirtualna(w przypadku środowisk wirtualnych jak Hyper-V, Vmware, Proxmox, AWS EC2) lub per maszyna fizyczna w przypadku fizycznych serwerów. Licencjonowanie powinno być realizowane w wariancie subskrypcji, w którym licencja ma określony termin ważności.
2	Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 50 chronionych zasobów jak maszyny wirtualne lub maszyny fizyczne.
4	W ramach dostawy wymagane jest dostarczenie licencji na ochronę 5 maszyn fizycznych z systemem operacyjnym Windows 10 Pro lub Ubuntu Desktop
5	Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska
III	Ochrona danych
1	Oprogramowanie musi posiadać funkcje backupu i replikacji:
a	Backup maszyn wirtualnych Vmware
b	Replikacja maszyn wirtualnych Vmware (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
c	Backup maszyn wirtualnych Hyper-V
d	Replikacja maszyn wirtualnych Hyper-V (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
e	Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
f	Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
g	Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
h	Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
i	Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych
j	Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem
k	Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
l	Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach
IV	Optimalizacja wykorzystania miejsca na dane

1	Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
a	Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
b	Kompresja backupu, w tym konfigurowalny stopień kompresji
c	Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne
V	Spójność danych
1	Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
a	Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
b	Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
c	Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji:
	Microsoft Exchange 2013, 2016, 2019
	Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022
d	Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
e	Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
f	Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
g	Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji
VI	Przywracanie danych
1	Oprogramowanie musi posiadać poniższe funkcje:
a	Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
b	Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)
c	Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
d	Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
	Microsoft Exchange
	MS Active Directory
	MS SQL
e	Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.
VI	
I	Wydajność
1	Oprogramowanie do backupu musi pozwalać na:
a	Tworzenie backupu i replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
b	Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
c	Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN
d	Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
e	Wsparcie dla urządzeń oferujących dodatkową deduplikację danych

VI	
II	Zarządzanie
1	Oprogramowanie musi pozwalać na następujące formy zarządzania:
a	Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
b	Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
c	Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania
d	Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.
e	Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
f	Oprogramowanie musi umożliwiać integrację z Active Directory
g	Oprogramowanie musi wspierać tzw. tryb multi tenant, umożliwiający podzielenie oprogramowania do backupu na kilka podinstancji zarządzanych z odrębnych interfejsów w celu rozłożenia zarządzania w złożonych środowiskach

Żłobek Miejski nr 1 w Pieszcach

I	Wymagania minimalne
1	Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji
a	Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012
b	Vmware vSphere min. w wersjach v5.5 - 9.0
c	Nutanix AHV v6.5, v6.10
d	Maszyny fizyczne: Windows Server 2025, 2022, 2019, 2016, 2012R2, 2012
e	Microsoft 365 (Exchange online, One Drive for Business, Sharepoint)
f	Proxmox Virtual Environment min. w wersji 8.0
2	Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V
3	Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:
a	na serwerze Windows lub Linux
b	jako maszyna wirtualna VMware
c	jako maszyna wirtualna Amazon
d	na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital
4	Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS
5	Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania
6.	Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
II	Licencjonowanie

1	Oprogramowanie powinno być licencjonowane per maszyna wirtualna(w przypadku środowisk wirtualnych jak Hyper-V, Vmware, Proxmox, AWS EC2) lub per maszyna fizyczna w przypadku fizycznych serwerów. Licencjonowanie powinno być realizowane w wariancie subskrypcji, w którym licencja ma określony termin ważności.
2	Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 50 chronionych zasobów jak maszyny wirtualne lub maszyny fizyczne.
4	W ramach dostawy wymagane jest dostarczenie licencji na ochronę 2 maszyn fizycznych z systemem operacyjnym Windows 10 Pro lub Ubuntu Desktop
5	Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska
III	Ochrona danych
1	Oprogramowanie musi posiadać funkcje backupu i replikacji:
a	Backup maszyn wirtualnych Vmware
b	Replikacja maszyn wirtualnych Vmware (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
c	Backup maszyn wirtualnych Hyper-V
d	Replikacja maszyn wirtualnych Hyper-V (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
e	Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
f	Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
g	Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
h	Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
i	Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych. Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem
j	Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
k	Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
l	Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach
IV	Optymalizacja wykorzystania miejsca na dane
1	Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
a	Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
b	Kompresja backupu, w tym konfigurowalny stopień kompresji
c	Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne
V	Spójność danych
1	Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:

a	Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
b	Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
c	Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji:
	Microsoft Exchange 2013, 2016, 2019
	Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022
d	Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
e	Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
f	Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
g	Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji
VI	Przywracanie danych
1	Oprogramowanie musi posiadać poniższe funkcje:
a	Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
b	Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)
c	Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
d	Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
	Microsoft Exchange
	MS Active Directory
	MS SQL
e	Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.
VI	
I	Wydajność
1	Oprogramowanie do backupu musi pozwalać na:
a	Tworzenie backupu i replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
b	Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
c	Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN
d	Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
e	Wsparcie dla urządzeń oferujących dodatkową deduplikację danych
VI	
II	Zarządzanie
1	Oprogramowanie musi pozwalać na następujące formy zarządzania:
a	Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
b	Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej

c	Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania
d	Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.
e	Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
f	Oprogramowanie musi umożliwiać integrację z Active Directory
g	Oprogramowanie musi wspierać tzw. tryb multi tenant, umożliwiający podzielenie oprogramowania do backupu na kilka podinstancji zarządzanych z odrębnych interfejsów w celu rozłożenia zarządzania w złożonych środowiskach

- usługa wdrożenia dostarczonych rozwiązań

Zamawiający wymaga realizacji następującego zakresu wdrożenia infrastruktury IT:

1. Serwer Fizyczny

- Montaż fizyczny:
 - Instalacja serwera (1) w szafie teleinformatycznej (rack).
 - Podłączenie serwera do zasilania, w tym do zasilacza awaryjnego (UPS), oraz do lokalnej sieci komputerowej (LAN).
- Podstawowa konfiguracja:
 - Wstępna konfiguracja interfejsu do zdalnego zarządzania serwerem.
 - Instalacja i aktywacja serwerowego systemu operacyjnego wraz z licencjami dostępnymi dla użytkowników.
 - Instalacja sterowników i wykonanie aktualizacji systemu operacyjnego.
 - Uruchomienie roli usługi katalogowej Active Directory.
 - Demonstracyjne utworzenie 3 kont użytkowników w usłudze katalogowej i przyłączenie trzech stacji roboczej do domeny.
 - Instalacja i konfiguracja oprogramowania do tworzenia kopii zapasowych.
 - Konfiguracja pilotażowego zadania tworzenia kopii zapasowych dla 3 stacji roboczych i 1 serwera.
 - Przygotowanie serwera pod instalację oprogramowania do zarządzania dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

2. Urządzenie brzegowe z funkcjonalnością UTM (brama sieciowa) 1 szt.

- Montaż fizyczny:
 - Montaż urządzenia w szafie rack.

- Podłączenie do zasilania oraz do sieci zewnętrznej (WAN) i wewnętrznej (LAN).
- Podstawowa konfiguracja:
 - Konfiguracja urządzenia jako głównej bramy internetowej.
 - Aktywacja podstawowych modułów bezpieczeństwa (UTM), takich jak zaporę sieciową (firewall), system antywirusowy i filtrowanie treści na domyślnych ustawieniach.
 - Ustawienie bazowych reguł zapory sieciowej w celu zabezpieczenia ruchu sieciowego.

3. Zarządzalny przełączniki sieciowe (4 szt.)

- Montaż fizyczny:
 - Montaż przełączników w szafie teleinformatycznej.
 - Podłączenie urządzeń do zasilania.
- Podstawowa konfiguracja:
 - Konfiguracja adresacji IP na potrzeby zarządzania przełącznikami.
 - Implementacja segmentacji sieci poprzez utworzenie 3 wirtualnych sieci lokalnych (VLAN) dla oddzielenia ruchu: administracyjnego, użytkowników oraz gości.
 - Przypisanie portów przełączników do odpowiednich sieci VLAN.

4. Punkty dostępne sieci bezprzewodowej (7 szt.):

- Montaż fizyczny:
 - Instalacja punktów dostępowych w uzgodnionych lokalizacjach w celu zapewnienia optymalnego zasięgu (zamawiający zapewni sieć infrastrukturalną oraz wszelkie prace przygotowawcze)
 - Podłączenie urządzeń do sieci LAN.
 - Podłączenie urządzeń do sieci elektrycznej (zamawiający zapewni dostęp do zasilania)
- Podstawowa konfiguracja:
 - Dodanie punktów dostępowych do centralnego systemu zarządzania (kontrolera sieci bezprzewodowej).
 - Konfiguracja i rozgłaszanie nazw sieci bezprzewodowych (SSID) powiązanych z odpowiednimi segmentami sieci (VLAN).

5. Zasilacz Awaryjny UPS

- Montaż fizyczny:

- Montaż jednostki UPS w szafie rack.
- Podłączenie urządzenia do sieci elektrycznej.
- Podłączenie serwera fizycznego do gniazd wyjściowych zasilacza UPS.
- Podstawowa konfiguracja:
 - Instalacja na serwerze oprogramowania do zarządzania zasilaczem UPS.
 - Skonfigurowanie podstawowych powiadomień oraz reguł automatycznego, bezpiecznego zamknięcia systemu operacyjnego serwera w przypadku utraty zasilania.

6. Oprogramowanie Klasy EDR/MDR

- Wdrożenie i konfiguracja:
 - Aktywacja licencji w konsoli zarządzającej dostawcy.
 - Konfiguracja dostępu do konsoli administracyjnej w chmurze.
 - Pilotażowe wdrożenie agentów oprogramowania na 3 stacjach roboczych i 1 serwerze.
 - Sprawdzenie poprawności komunikacji zainstalowanych agentów z konsolą centralną.

7. Wdrożenie i szkolenie z systemu SIEM

- Instalacja i konfiguracja:
 - Wykonawca przeprowadzi podstawowe wdrożenie systemu w zakresie niezbędnym do uruchomienia centralnego zbierania i agregowania logów.
 - Zakres prac obejmuje instalację i konfigurację komponentów centralnych systemu oraz podstawową konfigurację dostępu administracyjnego.
 - W ramach pilotażu wykonawca podłączy do systemu co najmniej 5 wskazanych urządzeń sieciowych poprzez konfigurację przesyłania logów.
 - W ramach pilotażu wykonawca zainstaluje i skonfiguruje agentów lub inne wymagane mechanizmy zbierania logów na co najmniej 5 wskazanych stacjach roboczych i/lub serwerach.
 - Wdrożenie obejmuje wyłącznie podstawową konfigurację systemu zbierania logów i nie obejmuje tworzenia rozbudowanych scenariuszy korelacyjnych, automatyzacji reakcji, playbooków, dedykowanych polityk bezpieczeństwa, rozbudowanych pulpitów menedżerskich ani innych niestandardowych rozszerzeń.
- Szkolenie:
 - Przeprowadzenie podstawowego instruktażu z obsługi interfejsu systemu SIEM, obejmującego przeglądanie zdarzeń i monitorowanie stanu podłączonych systemów.

PODSUMOWANIE OPISU PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI 1

Zamawiający wymaga, aby wszystkie oferowane urządzenia i sprzęt były fabrycznie nowe oraz pochodziły z autoryzowanych kanałów dystrybucji na terenie Polski. W przypadku oprogramowania, Zamawiający również oczekuje, że będzie ono pozyskiwane wyłącznie z oficjalnych źródeł dystrybucyjnych w kraju.

Dopuszcza się zastosowanie rozwiązań równoważnych. Jeżeli w dokumentacji przetargowej pojawiły się odniesienia do konkretnych nazw własnych, znaków towarowych, modeli, producentów lub pochodzenia produktów, należy traktować je jako określenie standardu jakościowego oraz oczekiwanego efektu końcowego. W takich przypadkach przyjęte parametry techniczne powinny być traktowane jako punkt odniesienia do minimalnych wymagań Zamawiającego.

Wykonawca ma prawo zaproponować materiały, urządzenia lub produkty równoważne, pod warunkiem, że spełniają one wymagane standardy jakościowe i funkcjonalne określone w dokumentacji postępowania. Zamawiający nie narzuca wyboru konkretnego producenta ani dostawcy, jednak proponowane rozwiązania muszą odpowiadać co najmniej standardom określonym w opisie przedmiotu zamówienia.

Pod pojęciem „rozwiązania równoważne” rozumie się produkty lub technologie, które pod względem parametrów technicznych, jakościowych i użytkowych nie odbiegają od wymagań określonych przez Zamawiającego. W przypadku zastosowania takiej alternatywy, Wykonawca zobowiązany jest wykazać, że proponowane rozwiązanie w pełni odpowiada oczekiwaniom postawionym w specyfikacji.

Jeżeli w opisie zamówienia wskazano konkretną markę, model, znak towarowy, producenta, patent, źródło pochodzenia lub charakterystyczny proces technologiczny, Zamawiający dopuszcza zastosowanie rozwiązań równoważnych. Warunkiem ich przyjęcia jest zachowanie parametrów technicznych, funkcjonalności użytkowej, trwałości oraz spełnienie wymagań dotyczących bezpieczeństwa użytkowania.