I.Zakup serwera Backup 1szt.

Przedmiotem zamówienia jest dostawa, instalacja (we wskazanym przez Zamawiającego punkcie), uruchomienie oraz konfiguracja serwera Backupowego wraz z oprogramowaniem do Backupu:

Wymagania dla serwera Backup:

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• serwerowa do montażu w szafie RACK 19" wysokości 2U • Obudowa powinna posiadać możliwość instalacji panelu LCD umieszczonego na froncie obudowy i pozwalającego jednoznacznie stwierdzić czy system działa poprawnie i pokazujący podstawowe stany działania serwera (umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze). • Obudowa z możliwością wyposażenia w kartę do bezpośredniej komunikacji z urządzeniem mobilnym. • 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. • W obudowie powinien być zainstalowany zestaw redundantnych wentylatorów.
Zasilanie	W obudowie powinien być zainstalowany zestaw redundantnych zasilaczy o mocy co najmniej 700W w standardzie Titanium każdy, wymienialnych podczas pracy
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • musi być wyposażona w zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust), • Musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o konfigurację wewnętrznego oprogramowania komponentów serwera. • Zintegrowany z płytą główną moduł TPM w wersji co najmniej 2.0
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach
Procesor	• Jeden procesor z uwagi na licencjonowanie posiadający minimum 16 rdzeni działający co najmniej z częstotliwością 3 GHz i dający w teście

	Passmark dostępnym na stronie https://www.cpubenchmark.net/ wynik nie mniejszy niż 43 300
RAM	• Na płycie głównej powinny znajdować się minimum 12 slotów przeznaczonych do instalacji pamięci taktowaną przynajmniej z częstotliwością 5600MT/s przy użyciu odpowiednich procesorów. • 128 GB pamięci RAM w modułach 64GB RDIMM przygotowanych na działanie z częstotliwością co najmniej 5600MT/s
Dyski twarde	• Serwer ma mieć zainstalowany moduł pozwalający na startowanie systemu z dysków M.2 NVMe skonfigurowanych w RAID1 nie zajmujących slotów na dyski, wymieniane podczas pracy systemu. • Miejsce na co najmniej 12 dysków w rozmiarze 3.5” wymienialne bez wyłączania systemu. • Zainstalowane co najmniej 7 dysków minimum 8TB Hot-plug
Kontroler RAID	• Serwer powinien posiadać kontroler RAID umożliwiający konfigurację RAID 0,1,5,10,50,6 posiadający co najmniej 8GB pamięci cache zabezpieczonej przed awarią prądu.
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie Base-T oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie Base-T (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Dodatkowo zainstalowane 4 porty 1GB Base-T
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panelu 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 • 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).
Kontroler eksploatacji serwera	Serwer powinien być standardowo wyposażony w kontroler eksploatacji Konfigurowanie ustawień BIOS i sprzętu. Uproszczoną instalację systemów operacyjnych z wbudowanymi sterownikami, z opcją instalacji bezobsługowej dla systemów Microsoft Windows i Red Hat Enterprise Linux 7. Aktualizację oprogramowania niezależnie od systemu operacyjnego, z możliwością przywrócenia poprzedniej wersji. Ciągłą dostępność diagnostyki bez zależności od dysku twardego, z automatyczną aktualizacją oprogramowania podczas wymiany komponentów. Usunięcie danych związanych z serwerem i pamięcią masową na wybranych komponentach. Możliwe jest usunięcie informacji z BIOS. Dostarczenie informacji o bieżącej i fabrycznej konfiguracji systemu. Udostępnianie logów sprzętowych w celu rozwiązywania problemów. Zdalne zarządzanie cyklem życia serwera co najmniej za pomocą interfejsu WS-Man Konfigurację ustawień sieci dla wbudowanej karty NIC, w tym ustawienia VLAN. Wykonywanie diagnostyki pamięci, urządzeń we/wy, procesora i dysków fizycznych. Aktualizację komponentów systemu za pomocą repozytoriów lub pojedynczych pakietów DUP. Powrót do poprzedniej wersji oprogramowania układowego. Umożliwia zabezpieczenie konfiguracji systemu - "System Configuration Lockdown mode" Automatyczną aktualizację oprogramowania i konfiguracji wymienionych części. Trwałe usunięcie danych przed ponownym wykorzystaniem lub wycofaniem systemu. Obsługę różnych metod aktualizacji, za pomocą różnych źródeł, takich jak FTP, udziały sieciowe (CIFS, NFS, HTTP, HTTPS) lub lokalne napędy USB/DVD
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ○ - zdalny dostęp do graficznego interfejsu Web karty zarządzającej ○ - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika ○ - możliwość podmontowania zdalnych wirtualnych napędów ○ - wirtualną konsolę z dostępem do myszy, klawiatury

	○ - wsparcie dla IPv6 - wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH ○ - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. ○ - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer ○ - integracja z Active Directory ○ - możliwość obsługi przez ośmiu administratorów jednocześnie ○ - Wsparcie dla automatycznej rejestracji DNS - wsparcie dla LLDP ○ - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej ○ - możliwość podłączenia lokalnego poprzez złącze RS-232. ○ - możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. ○ - Monitorowanie zużycia dysków SSD ○ - możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, ○ - Automatyczne zgłaszanie alertów do centrum serwisowego producenta ○ - Automatyczne update firmware dla wszystkich komponentów serwera ○ - Możliwość przywrócenia poprzednich wersji firmware ○ - Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.
Oprogramowanie do zarządzania	Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: - wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; - możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta; - wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH; - możliwość oskryptowywania procesu wykrywania urządzeń; - możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram; - szczegółowy opis wykrytych systemów oraz ich komponentów; - możliwość eksportu raportu do CSV, HTML, XLS; - grupowanie urządzeń w oparciu o kryteria użytkownika; - automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń; - szybki podgląd stanu środowiska; - podsumowanie stanu dla każdego urządzenia; - szczegółowy status urządzenia/elementu/komponentu; - generowanie alertów przy zmianie stanu urządzenia;

	- filtry raportów umożliwiające podgląd najważniejszych zdarzeń; - integracja z service desk producenta dostarczonej platformy sprzętowej; - możliwość przejęcia zdalnego pulpitu; - możliwość podmontowania wirtualnego napędu; - kreator umożliwiający dostosowanie akcji dla wybranych alertów; - możliwość importu plików MIB; - przesyłanie alertów „as-is" do innych konsol firm trzecich; - aktualizacja oparta o wybranie źródła bibliotek (lokalna, online producenta oferowanego rozwiązania); - możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta; - możliwość tworzenia ról administratorskich z różnym poziomem uprawnień np. oddzielna rola pozwalająca na aktualizację oprogramowania układowego. - możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów; - moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: o ilość podłączonych oraz rozłączonych systemów o stan podłączonych urządzeń o informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów o Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia o informacje o statusie gwarancji dla poszczególnych urządzeń o informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń o informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. o Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych o 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 systemy 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: ▪ 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 anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów

	▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware o możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty o Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, o Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji o Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo o 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. o Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. o Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.

	○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ 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 ○ 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 ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. Inne: • Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Aplikacja do zarządzania	Aplikacja mobilna do zarządzania serwerami powinna umożliwiać: • Monitorowanie stanu serwerów, w tym odczyt parametrów zdrowia, inwentarza i konfiguracji. • Konfigurowanie ustawień serwera, takich jak parametry sieci, hasła administratora i kolejność urządzeń rozruchowych. • Bezpośrednią komunikację z kontrolerem serwera za pomocą technologii bezprzewodowej. • Zdalne zarządzanie serwerami poprzez połączenie z konsolą zarządzania. • Pobieranie informacji o serwerach takich jak inwentarz, status, alerty oraz logi. • Konfigurowanie serwerów zdalnie. • Wysyłanie poleceń sterowania zasilaniem i innych poleceń. • Otrzymywanie powiadomień o alertach z systemów zarządzania. • Pobieranie informacji o gwarancji. • Uruchamianie zewnętrznych aplikacji, takich jak klienty zdalnego pulpitu. • Zabezpieczenie danych w aplikacji poprzez szyfrowanie z użyciem klucza specyficznego dla urządzenia. • Opcjonalne zabezpieczenie dostępu do aplikacji za pomocą hasła i biometrii. • Automatyczne wylogowanie w przypadku braku aktywności. • Połączenie z serwerami za pomocą technologii Bluetooth Low Energy (BLE) lub Wi-Fi. • Wyświetlanie szczegółowych informacji o serwerze oraz dzienników. • Otrzymywanie automatycznych powiadomień z konsoli zarządzania. • Przypisywanie adresów IP i modyfikowanie haseł. • Konfigurowanie atrybutów BIOS. • Wyłączanie i włączanie serwera oraz dostęp do konsoli systemowej.

	• Pobieranie danych z systemów zarządzania typu "jeden do wielu". • Wyświetlanie certyfikatu systemu w celu weryfikacji tożsamości przy pierwszym połączeniu. Aplikacja powinna być dostępna do pobrania w popularnych sklepach z aplikacjami • Kryterium stanowi dodatkową punktację.
Opcjonalny moduł do podłączenia aplikacji mobilnej	Moduł powinien umożliwiać następujące funkcjonalności: • Bezprzewodową komunikację z urządzeniami mobilnymi wykorzystując technologie Bluetooth Low Energy (BLE) lub Wi-Fi. • Zapewnienie fizycznego bezpieczeństwa poprzez wymóg fizycznej obecności administratora przy serwerze i naciśnięcia przycisku aktywacyjnego na serwerze lub wirtualnego przycisku na wyświetlaczu LCD w przypadku obudów. Bez aktywacji nie jest możliwa wymiana danych. • Ograniczenie zasięgu komunikacji BLE przed uwierzytelnieniem do około 1 metra, a po uwierzytelnieniu do około 5 metrów. Zasięg Wi-Fi wynosi około 5 metrów. • Ograniczenie liczby jednoczesnych połączeń BLE do jednego urządzenia mobilnego na serwer. • Blokowanie dostępu po wielokrotnych próbach połączenia z użyciem nieprawidłowych danych uwierzytelniających, co skutkuje koniecznością ręcznej reaktywacji modułu. • Zabezpieczenie komunikacji BLE z wykorzystaniem protokołu TLS 1.2, wymiany kluczy Diffie-Hellmana (2048-bitowe lub większe liczby pierwsze) oraz szyfrowania AES (128-bitowe klucze symetryczne). • Wykorzystanie trybu szyfrowania GCM z unikalnymi numerami sekwencyjnymi w celu ochrony przed nieautoryzowaną ingerencją, ujawnieniem informacji oraz atakami typu replay. • Aktywację Wi-Fi tylko w przypadku komunikacji wymagającej większej przepustowości lub komunikacji opartej na IP. • Generowanie nowego, losowego klucza WPA2PSK za każdym razem, gdy aktywowane jest Wi-Fi, który jest przesyłany do aplikacji mobilnej za pośrednictwem połączenia BLE. • Uwierzytelnianie użytkowników za pomocą tych samych danych uwierzytelniających co do kontrolera zdalnego dostępu. • Identyfikację serwera za pomocą certyfikatu PKI w formacie x509 oraz wyświetlanie znacznika serwisowego podczas łączenia. • Możliwość aktywacji diody ID LED w celu potwierdzenia połączenia z właściwym systemem. • Umożliwienie administratorom zdalnego wyłączania i włączania serwerów za pomocą poleceń.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • 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 Polski według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.**
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim wraz z tłumaczeniem na język polski. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres zgodny z zaproponowanym w formularzu ofertowym. • W przypadku awarii dysku, uszkodzony pozostaje u klienta • 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 wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
	• Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
	  ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
	  ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.
	  ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.
	  ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.
	  ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i 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.
	• Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
	
	Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

System operacyjny	Na serwerze musi być zainstalowany fabrycznie nowy, oryginalny system Windows Server 2025 Standard (licencja obejmująca min. 16 rdzeni) w polskiej wersji językowej. Dopuszcza się licencję OEM z kluczem zapisanym w BIOS/UEFI lub licencję wieczystą dostarczoną wraz z certyfikatem autentyczności i dowodem zakupu.

	System musi posiadać prawo do obniżenia wersji (downgrade) do Windows Server 2019 Standard. Wykonawca zobowiązany jest dostarczyć klucz produktu oraz obraz systemu dla wersji docelowej (2025) oraz wersji downgrade (2019). Dostawca musi zapewnić narzędzia lub nośnik (np. USB/ISO) umożliwiający przywrócenie systemu do stanu fabrycznego. Wybór systemu operacyjnego jest podyktowany bezkonfliktową współpracą z istniejącą infrastrukturą informatyczną w urzędzie oraz z oprogramowaniem firm trzecich wykorzystywanym do codziennej pracy.

Wymagania dla oprogramowania do backupu:

Wymagania ogólne
Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner Peer Insights: i spełniać minimalne wymaganie: - minimalna liczba referencji 500, - minimalna ocena z referencji 4,6.
Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x, 8.x i 9.0 oraz Microsoft Hyper-V 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne dla powyższych platform wirtualizacyjnych, chyba, że wyszczególniono inaczej
Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.8.x - 7.3, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.5 lub nowszy, Proxmox VE 8.2, 8.3, 8.4 lub 9.0 oraz Scale Computing HyperCore 9.4.32.218226 – 9.5.x.
Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
System backupowy musi mieć możliwość wdrożenia wszystkich komponentów (np. serwer backupowy, serwer pośredniczący, repozytorium) na platformach Windows oraz Linux
System backupowy musi mieć możliwość wdrożenia w oparciu o tzw. appliance zgodny z wytycznymi bezpieczeństwa DISA (Defense Information Systems Agency)
Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków

Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć wiele wirtualnych puli pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej 20 pamięci masowych w pojedynczej puli.
Oprogramowanie musi pozwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta.
Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage, IBM Cloud Storage, 11:11 Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania do backupu oraz odtwarzania obrazu maszyny wirtualnej
Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
Oprogramowanie musi umożliwiać tworzenie logicznie odseparowanych środowisk dla różnych organizacji/działów. Dodatkowo system musi wspierać kontrolę dostępu w oparciu o role (RBAC) - predefiniowane lub własne
Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
Oprogramowanie musi umożliwiać integracje z różnymi dostarczycielami tożsamości (IdP - Identity Providers) z wykorzystaniem protokołu SAML (np. Entra ID, Okta)
Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora, reset zablokowanego konta)
Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS)
Oprogramowanie musi posiadać integracje z systemami typu SIEM

Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej oraz analizy istniejącej instalacji systemu backupowego. Powinna istnieć możliwość wyłączenia tej opcji.
Oprogramowanie musi pozwalać na wydawanie komend głosowych asystentowi AI
Wymagania RPO
Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna conajmniej dla platformy VMware i Hyper-V
Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).
Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 - 2025 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere lub dowolnego systemu operacyjnego Windows Server 2016-2025 (z innych platfrom - fizycznych, wirtualnych, chmurowych). Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
Wymagania RTO

Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
Dodatkowo dla środowiska vSphere, Hyper-V, Nutanix AHV i MS Azure powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w platformę. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny, zarówno fizycznej jak i wirtualnej
Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
Oprogramowanie musi wspierać bezagentowy backup, spójny aplikacyjnie (tzw. Application Consistent) dla maszyn wirtualnych z platfrom vSphere, Hyper-V, Nutanix AHV, Proxmox.
Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej (Minimum dla Active Directory, MS Exchange, MS SQL, MS Sharepoint, Oracle i PostgreSQL).
Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects oraz pozwalać na odtworzenie haseł.
Oprogramowanie musi pozwalać na backup i odtwarzanie usługi Entra ID. W szczególności użytkowników, grupy, role, jednostki administracyjne, entrprise applications, Conditional Access Policies, Intune Policies oraz logi audytowe i sign-in.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2
Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Ograniczenie ryzyka
Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych
Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych.

Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
Oprogramowanie musi posiadać swój wbudowany program antywirusowy zoptymalizowany do przeszukiwania kopii backpowych
Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware
Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania
Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków
Oprogramowanie musi posiadać mechanizm wykrywania oznak ataku hakerskiego tzw Indicators of Compromise
Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR/XSIAM, CrowdStrike Falcon LogScale, Microsoft Sentinel.
Środowiska fizyczne
Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Rocky Linux, AlmaLinux
Rozwiązanie musi wspierać system operacyjny macOS
Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
Rozwiązanie musi wspierać backup podłączonych dysków USB
Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)

Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
Rozwiązanie musi wspierać kontrolę pasma sieciowego
Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
Rozwiązanie musi wspierać technologię BitLocker
Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange, Microsoft Active Directory, Microsoft Sharepoint, Microsoft SQL, Oracle, PostgreSQL oraz MongoDB
Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle i PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform
Rozwiązanie musi wspierać szyfrowanie
Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
Rozwiązanie musi wspierać tworzenie wielu zadań backupowych

II. Zakup licencji na oprogramowanie do monitorowania infrastruktury informatycznej 1szt.

Przedmiotem zamówienia jest dostawa oprogramowania do monitorowania infrastruktury informatycznej umożliwiające monitoring, min. 40 urządzeń (komputery, serwery).

Wymagania:

Oprogramowanie musi posiadać budowę modułową, składającą się z serwera zarządzającego, zdalnych konsoli oraz Agentów.
Instalacje zdalnych konsoli zarządzania nie podlegają limitom i nie są objęte dodatkowym

licencjonowaniem.
Komunikacja pomiędzy Serwerem a Agentami i Konsolami powinna nawiązywana być przy użyciu szyfrowanego protokołu TLS 1.3.

Moduły mają umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem.

Baza danych Programu musi być bezpłatna.

Oprogramowanie powinno zawiera rozbudowany system raportowy w tym minimum 130 raportów predefiniowanych
Powinien umożliwiać tworzenie własnych raportów wraz z możliwością pełnego dostosowania wyglądu oraz przywrócenia bazowej konfiguracji raportów wbudowanych po ich edycji.
Dane, które dotyczą działań pracownika na komputerze, takie jak: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., muszą być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej.
Muszą pozwalać na usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.

Dostęp do danych osobowych oraz danych z monitoringu, musi objęty być kontrolą.

W programie musi być możliwość nadawania kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator ma mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Administratorzy, którzy nie mają pełnych praw nie mogą widzieć się w konsoli zarządzania.

Program musi posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in.:

- logowanie dostępu do Opcji programu,
- logowanie dostępu do informacji o aktywności użytkownika,
- logowanie poleceń deinstalacji Agenta.

Działania administratorów powinny być automatycznie eksportowane do zewnętrznego kolektora Syslog.

Lista kont użytkowników, w tym administratorów, musi możliwość synchronizowana z Active Directory wraz z awatarami oraz dowolnymi atrybutami, również przez szyfrowane połączenie LDAPS.
Program powinien umożliwiać również tworzenie lokalnych kont użytkowników wraz z awatarami w środowiskach bez Active Directory.
Liczba kont użytkowników w konsoli nie może być objęta limitem i nie podlegać licencjonowaniu.

Program musi wspierać konfigurację polityki haseł do lokalnych kont użytkowników konsoli.

Program musi zawierać mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny powinien być móc oznaczony czasem ważności i redystrybuowany za pomocą e-mail i/lub SMS.

Monitorowanie infrastruktury (bezagentowo) musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

- wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
- wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)
- wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
- wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako
- tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
- wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach w dowolnym rozmiarze i kolorze
- wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
- wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny
- zablokowania mapy urządzeń przed przypadkową edycją
- serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych
- serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów
- serwerów pocztowych:
  - program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty
  - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem)
  - program ma możliwość wykonywania operacji testowych
  - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa
- monitorowania serwerów WWW i adresów URL
- cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
- obsługi szyfrowania TLS w powiadomieniach e-mail
- obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID

- obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
- monitoringu routerów i przełączników wg:
  - zmian stanu interfejsów sieciowych
  - ruchu sieciowego
  - podłączonych stacji roboczych – graficzna prezentacja panelu switcha
  - ruchu generowanego przez podłączone do portów stacje robocze
- serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
- wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
- monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano
- zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny
- wydajności systemów Windows: obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

Program musi posiadać inteligentne mapy, oraz umożliwiać tworzenie dynamicznych map wg własnych filtrów.
Program musi posiadać kryteria automatycznego filtrowania m.in.:
- statusu Agenta,
- wygenerowanych alarmów,
- zainstalowanych aplikacji,
- przynależności do oddziału,
- serwisów sieciowych,
- danych z SNMP,
- danych z inwentaryzacji urządzenia itp.

Program musi posiadać funkcję kompilatora plików MIB

Program musi umożliwiać nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.:
- wysłanie komunikatu pulpitowego,
- wysłanie wiadomości e-mail,
- wysłanie SMS,
- wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl,
- wysłanie wiadomości przez Microsoft Teams (poprzez mechanizmy webhook i workflow) oraz Slack,
- uruchomienie programu,
- wysłanie pułapki SNMP,
- wysłanie pakietu Wake-On-LAN,
- zatrzymanie/restart usługi Windows,
- wyłączenie/restart komputera.

Program musi mieć możliwość budowana alarmów z wykorzystaniem ciągu przyczynowo skutkowego. Wykonywanie akcji alarmów musi być konfigurowalne, w tym po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut.
Dla akcji musi być możliwość nałożenia ograniczeń czasowych

Alarmy muszą pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia.

Oprogramowanie musi umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0

Program musi mieć możliwość integracji ze sprzętową bramką GSM HW-SMS-GW 3

Program automatycznie musi gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

1. Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
2. Umożliwiać odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.
3. Obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
4. Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows.
5. Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
6. Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
7. Umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
8. Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
9. Umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
10. Umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
11. Umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.

Program musi wspierać inwentaryzacje zasobów - prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i oprogramowania:

- ✓ przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
- ✓ przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów,
- ✓ tworzenia powiązań między zasobami a urządzeniami,

- ✓ tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak
- ✓ i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
- ✓ tworzenia relacji pomiędzy zasobami,
- ✓ wskazania osób uprawnionych do użycia zasobów,
- ✓ definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości
  dla danego urządzenia lub oprogramowania musi istnieć możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
- ✓ określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
- ✓ określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
- ✓ masową edycję atrybutów zasobów,
- ✓ definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
- ✓ importu danych z zewnętrznego źródła min.: .CSV,
- ✓ przechowywania dowolnych dokumentów min:. pliki .DOCX, .XLSX, .PDF,
- ✓ kopiowanie powielanie zasobów z możliwością wyboru atrybutów do powielenia,
- ✓ automatyczne nadawanie numeru inwentarzowego do powielanych zasobów,
- ✓ tworzenia powiązań między zasobami a dokumentami,
- ✓ oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
- ✓ ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
- ✓ generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
- ✓ przygotowania wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
- ✓ konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
- ✓ konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
- ✓ archiwizacji i porównywania audytów zasobów,
- ✓ tworzenia kodów kreskowych dla zasobów,
- ✓ drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
- ✓ inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i

edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,

- ✓ możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
- ✓ inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
- ✓ definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data" z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja")
- ✓ powiązania zgłoszeń w module pomocy użytkownikom z zasobami.

Oprogramowanie ma zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie
2. archiwów ZIP.
3. Informacje o aplikacjach używanych w organizacji.
4. Tworzenie własnych wzorców aplikacji.
5. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
6. Informacje o komputerach, na których aplikacja została wykryta.
7. Zarządzanie posiadanymi licencjami.
8. Wskazywanie osób odpowiedzialnych za licencję.
9. Wskazanie użytkowników licencji.
10. Tworzenia powiązań między licencjami a dokumentami w relacji 1 do wielu.
11. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
12. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
13. Zarządzanie posiadanymi licencjami: raport zgodności licencji.
14. Możliwość przypisania do programów numerów seryjnych, wartości itp. Okna audytowe posiadają możliwość filtrowania elementów per oddział.

Program musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

- ✓ Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
- ✓ Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz
- ✓ informacją o uruchomieniu na podwyższonych uprawnieniach,
- ✓ Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
- ✓ Informacji o edytowanych przez użytkownika dokumentach,
- ✓ Historii pracy (cykliczne zrzuty ekranowe),

- ✓ Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),
- ✓ Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
- ✓ Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
- ✓ Nagłówków przesyłanej w aplikacjach klienckich poczty email,
- ✓ Wykrywania podejrzanej aktywności przez popularne „jigglery", mającej na celu symulowanie faktycznej pracy.
- ✓ Zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.
- ✓ Wyszczególnienia podejrzanej aktywności w raportach.
- ✓ Wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności.
- ✓ Alarmowania o aktywności użytkownika poza zdefiniowanymi godzinami pracy.
- ✓ Automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności.
- ✓ Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami.
- ✓ Integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT.
- ✓ Skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia.
- ✓ Automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych.
- ✓ Blokowania ruchu na wskazanych portach TCP/IP,
- ✓ Blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
- ✓ Prowadzenia rejestru naruszeń blokad,
- ✓ Wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,
- ✓ Przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
- ✓ Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.

Program musi mieć możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.
Program ma umożliwiać realizację zdalnej pomocy użytkownikom. W ramach kontroli stacji użytkownika musi być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i

opcją odrzucenia takiego połącznia przez użytkownika.

Funkcja zdalnego dostępu ma oferować możliwość zasłonienia ekranu przed użytkownikiem w taki sposób, aby nie widział czynności wykonywanych przez administratora.
Zdalne połączenie musi być możliwe również do komputerów, które nie posiadają ekranów (maszyny wirtualne, komputery bez podłączonego monitora lub laptopy z zamkniętym skrzydłem matrycy).
Program ma zawierać bazę zgłoszeń i umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, z przyporządkowywaniem odpowiednim administratorom, otrzymującym powiadomienie o problemie. Program musi pozwalać na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. oraz umożliwiać przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach")
Program ma umożliwiać użytkownikom monitorowanie procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, oraz zapewnić komunikację dwustronną.

Program musi wspierać proces ochrony przed wyciekiem danych poprzez:

1. Blokowanie urządzeń i nośników danych.
2. Program ma mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
3. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
4. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
5. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
6. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
9. Tworzenie list (map) komputerów, które zostały już zaszyfrowane, lub jeszcze nie zostały zaszyfrowane.
10. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.
11. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
12. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich
13. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Program ma mieć funkcjonalność umożliwiającą zarządzanie prawami dostępu do urządzeń i audyt operacji na plikach w tym:

1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
2. Autoryzowanie urządzeń firmowych/prywatnych (przykładowo szyfrowanych): pendrive'ów, dysków itp.
3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.

4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.
6. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
7. Podłączenie/odłączenie urządzenia przenośnego.
8. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.
9. Definiowanie reguł monitorowanych folderów w postaci list.
10. Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych

Program musi zapewnić integracje z Active Directory poprzez zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.
Program ma umożliwiać prowadzenie rejestru naruszeń blokad podłączanych nośników.
Program musi posiadać Portal informacyjny w formie platformy WWW oraz pozwalać na tworzenie wielu interaktywnych paneli informacyjnych z responsywnymi widgetami, których nazwy można zmieniać wg potrzeb.
Program musi być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.
Instalator programu musi być zabezpieczony podpisem cyfrowym wystawionym i zweryfikowanym przez zaufany globalny urząd certyfikacji (CA).
Program musi być dostępny jest w języku polskim,
Wsparcie techniczne musi być świadczone telefonicznie lub mailowo w języku polskim

III.Zakup licencji na urządzenie UTM

Przedmiotem zamówienia jest przedłużenie licencji bezpieczeństwa dla posiadanego przez Zamawiającego urządzenia UTM Check Point Quantum Spark 1590WL Appliance.

Licencja musi zawierać następujące moduły bezpieczeństwa:

- Firewall
- VPN (IPsec)
- IPS
- Application Control
- Content Awareness
- URL Filtering
- Anti-bot
- Anti-Virus
- Anti-Spam
- SandBlast Threat Emulation
- SandBlast Threat Extraction

Okres ważności licencji: Licencja musi być ważna do dnia 30.06.2026 r.
Wymagania dodatkowe:

- Licencja musi być w pełni kompatybilna z posiadanym urządzeniem Check Point Quantum Spark 1590 Appliance.
- Zamawiający wymaga dostarczenia licencji w formie elektronicznej (kod aktywacyjny lub plik licencyjny) wraz z instrukcją aktywacji.

- Wraz z licencją należy zapewnić dostęp do aktualizacji sygnatur oraz wsparcia technicznego producenta przez cały okres jej obowiązywania.
- Wsparciem serwisowy musi być też objęte samo urządzenie.

IV.Zakup dysków do posiadanego serwera (2 szt.)

Dostawa 2 sztuk dysków twardych SAS o pojemności 4TB każdy, przeznaczonych do rozbudowy przestrzeni backupowej w posiadanym przez Zamawiającego serwerze Dell PowerEdge R350.
Model referencyjny (obecnie wykorzystywany): Dell 10N7R 4TB 7.2K NL SAS 12Gbps 512n 3.5" Hot-Plug Hard Drive with Tray

Oferowane dyski muszą być fabrycznie nowe, nieużywane.
Gwarancja realizowana przez producenta na okres zgodny z zaproponowanym w formularzu ofertowym.
Dodatkowe wymagania i sposób weryfikacji:
Wykonawca jest zobowiązany do podania w ofercie dokładnego numeru części Dell (Dell Part Number / DP/N) oferowanego dysku.

V.Zakup zasilania awaryjnego UPS stanowiskowych 5 szt.

Przedmiotem zamówienia jest dostawa 5 szt. UPS-ów stanowiskowych o następujących parametrach:

Typ obudowy: Tower
Wyświetlacz: LCD
Moc pozorna: Min. 800 VA
Moc czynna: min. 450 W
Architektura UPS-a: line-interactive
Liczba faz na wejściu:1 (230V)
Liczba akumulatorów:1
Napięcie:230 V
Wbudowany układ stabilizacji napięcia AVR
Automatyczny restart po przywróceniu zasilania sieciowego
Ładowanie w trybie wyłączonym
Funkcja "zimnego startu"
Funkcja oszczędzania energii
Pojemność akumulatora: min. 9 Ah
Czas przełączenia (maks.) <9 ms
Czas transferu (maks.)<8,5 ms
Czas podtrzymania (obciążenie 100%) min.: 0.1 min
Czas ładowania: max 7h
Zabezpieczenia / filtry:

- Nadmierne rozładowanie

- Przeciwprzepięciowe
- Przeciwzwarciowe
- Przeciw przeładowaniu
- Termiczne

Darmowe Oprogramowanie do monitorowania pracy UPS w języku Polskim
Złącza:

- RJ-11
- RJ-45
- 1 x USB (Typ B)

Wymiary: nie większe niż148 x 305 x 120 mm.
Regulacja częstotliwości wyjściowej: Modyfikowana sinusoida Hz

VI.Zakup zarządzalnych Access Pointów 2 szt.

Przedmiotem zamówienia jest dostawa, instalacja uruchomienie oraz konfiguracja (według wytycznych Zamawiającego) 2 punktów dostępowych (AP) sieci WiFi. Każdy z punktów dostępowych musi spełniać wymagania i parametry techniczne określone w poniższym opisie.

Minimalne wymagania funkcjonalne punktu dostępowego (AP):

Parametry wymagane:

1. Punkt dostępowy przeznaczony do montażu wewnątrz budynków, wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 2.4GHz i 5 GHz.

- Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym (bez nadzoru centralnego kontrolera),
- Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej (oferowanym w ramach niniejszego postępowania),
- Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https,
- Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki.

2. Parametry fizyczne:
   - temperatura pracy: -10º do +50ºC,
   - wilgotność pracy: 5% - 90%,
   - Pamięć flash minimum 256MB,
   - Możliwość podłączenia zewnętrznego zasila-cza DC 12V,
   - Minimum 1 port RJ-45 100M/1000M/2500 Mbit/s auto-sensing PoE IN (z możliwością zasilania w technologii PoE+),
   - Port USB umożliwiający instalację modułu IoT,
   - Obsługa BLE w wersji 5.4,
   - Waga urządzenia nie większa niż 0,5 kg,
   - Przycisk przywracający konfigurację fabryczną,
   - Slot zabezpieczający typu Kensingston,

- Zużycie energii: nie więcej niż 14W.

3. Funkcjonalność:

- Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP,
- Wsparcie dla standardów bezpieczeństwa: WPA, WPA2, WPA3, WPA2-PPSK, 802.1x,
- 802.11w, DHCP Snooping, Dynamic ARP Inspection (DAI) lub równoważny, IP Source Guard (IPSG) lub równoważny oraz tworzenie ACL,
- Wsparcie dla roamingu zgodnego z 802.11k, 802.11v, 802.11r,
- Obsługa 256 równocześnie podłączonych użytkowników do punktu dostępowego,
- Wydajność 689 Mbps dla 2.4GHz oraz 2,88 Gbps dla 5GHz,
- Kompatybilność dla protokołów oraz standardów sieciowych takich jak: IPv6, SAVI IPv6, 802.1q, 802.3ab, LLDP, MDI, MDI-X, mDNS, NAT, GRE,
- Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą mechanizmów autoadaptacyjnych,
- Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punk-tów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe,
- Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu,
- Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma,
- Wykrywanie interferencji oraz miejsc bez po-krycia sygnału,
- Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach:
- EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-CHAP, EAP-SIM, EAP-AKA, EAP-GTC,
- EAP-FAST, EAP-PEAP, EAP-MD5, EAP-MSCHAPv2, PEAPv0, PEAPv1,
- Funkcjonalność szyfrowania komunikacji pomiędzy Access pointem a kontrolerem,
- Wbudowane dwuzakresowe inteligentne anteny typu smart „smart antena”, konstrukcja pomaga zapewnić optymalny kierunek zasięgu sygnału i jakość sygnału dla każdej mobilnej stacji dostępowej. Algorytm wykrywa gęstość dostępu osiągając dokładniejszy zasięg sygnału i tłumienie zakłóceń,
- Obsługa monitoringu przez SNMP,
- Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT,
- Certyfikaty dotyczące bezpieczeństwa: UL 60950-1, EN 60950-1.

4. Wraz z urządzeniami muszą zostać dostarczone: pełna dokumentacja w języku polskim, dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana.
5. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
6. Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich

osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.

7. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń
8. Zamawiający wymaga, aby punkty dostępowe posiadały serwis gwarancyjny świadczony przez Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń na okres zgodny z zaproponowanym w formularzu ofertowym. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).
9. W celu zapewnienia odpowiedniego poziomu świadczonych usług Wykonawca/autoryzowany serwis producenta musi posiadać status autoryzowanego partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim.
10. Producent oferowanych urządzeń musi znajdować się w kwadracie „Leaders" raportu Gartner pt. „Magic Quadrant for Enterprise Wired and Wireless LAN" za rok 2025 r. lub równoważnym. Jako ranking równo-ważny Zamawiający uzna ranking klasyfikujący rozwią-zania enterprise przewodowych i bezprzewodowych sieci LAN, prowadzony i publikowany przez podmiot niezależny od producentów tych rozwiązań. Zamawiający wymaga, aby ranking taki był aktualizowany w okresach nie dłuższych niż 1 rok. Podstawą do sporządzenia raportów muszą być badania polegające na sprawdzeniu jakości oferowanych usług i rozwiązań. Ranking równoważny nie może być wystawiony przez Wykonawcę lub podmiot zależny od Wykonawcy.

VII. Zakup przełączników zarządzalnych - 2 szt.

Przedmiotem zamówienia jest dostawa, instalacja (we wskazanym przez Zamawiającego punkcie), uruchomienie oraz konfiguracja (według wytycznych Zamawiającego) 2 przełączników sieciowych dla sieci LAN.
Każdy z przełączników sieciowych musi spełniać wymagania i parametry techniczne określone w poniższym opisie.

Minimalne wymagania funkcjonalne przełącznika sieciowego:

Parametry wymagane:

1. Przełącznik drugiej i trzeciej warstwy modelu ISO/OS.
   Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie RACK.
2. Wymagane parametry fizyczne:
   - możliwość montażu w stelażu/szafie 19",
   - wysokość maksymalna 1U,
   - zakres temperatur pracy ciągłej co najmniej od -5 °C do +50 °C,
   - zakres wilgotności pracy co najmniej 5% - 95%,

- waga urządzenia nie większa niż 6,5 kg,
- głębokość urządzenia maksymalnie 42 cm.

3. Przełącznik musi posiadać minimum:
   - 48 portów 10M/100M/1GE ze wsparciem dla funkcjonalności PoE 802.3af i 802.3at,
   - Minimalny budżet mocy PoE 846 W,
   - Wbudowany pojedynczy zasilacz,
   - 4 porty 10GE SFP+,
   - 2 dedykowane porty do łączenia przełączników w stos. Porty nie mogą być współdzielone z wymaganymi 4 portami 10GE SFP+,
   - Port konsoli RS232 ze złączem RJ45,
   - Port USB umożliwiający podłączenie zewnętrznej pamięci flash.

4. Maksymalny pobór mocy przez przełącznik przy nieaktywnej funkcjonalności PoE – 77W.

5. Funkcje PoE:
   - Perpetual PoE – podtrzymywanie zasilania dla podłączonych urządzeń podczas restartu przełącznika,
   - Fast PoE – po przywróceniu zasilania przełącznik zaczyna dostarczać moc do punktów końcowych bez czekania na pełne załadowanie systemu operacyjnego przełącznika, co przyspiesza uruchomienie podłączonych urządzeń PoE (kamery, AP, etc.).

6. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:
   - Zarządzanie stosem poprzez jeden adres IP,
   - Możliwość łączenia min. 9 jednostek w stos,
   - Magistrala stackująca o wydajności minimum 80 Gb/s,
   - Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. crossstack link aggregation),
   - Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree.
7. Układ przełączający o wydajności min. 224 Gbps,
8. Wydajność przełączania przynajmniej 168Mpps.
9. Obsługa min. 32 000 adresów MAC.
10. Wbudowana pamięć RAM min. 2GB.10.
11. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1GB.
12. Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ).
13. Voice VLAN, Guest VLAN.
14. Obsługa ramek jumbo o wielkości min. 9216 bajtów.
15. Obsługa mechanizmów: ERPS: G.8032 v2.
16. Obsługa protokołów: BFD, LACP, VRRP, LLDP.
17. Wsparcie dla protokołów: 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).
18. Wsparcie dla mechanizmu PVST lub równoważnego (innego niż wymagany standard STP/RSTP/MSTP).
19. Obsługa protokołów routingu dynamicznego: RIP, RIPng, OSPFv2, OSPFv3, VRRPv4, VRRPv6,
20. Wsparcie dla routingu statycznego: Policy based routing (PBR).
21. Obsługa min. 4096 tras dla routingu IPv4, Obsługa min. 1024 tras dla routingu IPv6.
22. Obsługa protokołów związanych z obsługą ruchu typu multicast:

- IGMP v1, v2 i v3,
- IGMP Snooping v1, v2 i v3,
- PIM-SM, PIM-DM, PIM-SSM.

23. Przełącznik musi być zgodny z IEEE 802.3az.
24. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client.
25. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    - min. 4 poziomy dostępu administracyjnego poprzez konsolę,
    - autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL,
    - obsługa sprzętowa reguł ACL. Możliwość utworzenia minimum 2000 reguł ACL,
    - możliwość uwierzytelniania urządzeń na por-cie w oparciu o adres MAC,
    - zarządzanie urządzeniem z wykorzystaniem protokołów HTTPS, SNMPv3 i SSHv2,
    - możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP,
    - obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard,
    - obsługa mechanizmów związanych z ochroną protokołu STP: BPDU Protection, Root Protection, Loop Protection,
    - możliwość synchronizacji czasu zgodnie z NTP IPv4 i IPv6,
    - możliwość uwierzytelnienia wielu użytkowników na jednym porcie z możliwością przydzielenia różnych VLANów dla każdego użytkownika z osobna,
    - Wsparcie dla protokołu Radius

26. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:
    - klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP,
    - wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WDRR, DRR oraz możliwość kolejkowania z bezwzględnym priorytetem „Strict Priority”.

    - Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów.
    - Wymagane opcje zarządzania:
    - możliwość lokalnej obserwacji ruchu na określonym porcie,
    - plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC),
    - możliwość zarządzania urządzeniem z wykorzystaniem protokołu Netconf/Yang lub RESTCONF,
    - wsparcie dla skryptów Python uruchamianych na urządzeniu,
    - wsparcie dla RMON.

27. Przełącznik musi mieć opcję szybkiego przywrócenie konfiguracji do poprzedniej wersji (tzw. funkcjonalność rollback). Przywrócenie konfiguracji do poprzedniej wersji nie może wymagać restartu urządzenia (całego bądź częściowego) bądź ręcznego odwoływania konfiguracji.

Administrator systemu musi mieć możliwość utworzenia znacznika/etykiety dla danej konfiguracji tak aby podczas wykonywania procesu przywrócenia można było wskazać ustawiony wcześniej znacznik/etykietę jako punkt, do którego ma zostać przy-wrócona konfiguracja.

28. Wraz z urządzeniami muszą zostać dostarczone:
    - pełna dokumentacja w języku polskim,
    - dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana.

29. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
30. Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.
31. Zamawiający wymaga, aby przełączniki posiadały serwis gwarancyjny świadczony przez autoryzowany serwis na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń na okres zgodny z zaproponowanym w formularzu ofertowym. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).
32. W celu zapewnienia odpowiedniego poziomu świadczonych usług autoryzowany serwis producenta musi posiadać status autoryzowanego partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim
33. Producent oferowanych urządzeń musi znajdować się w kwadracie „Leaders" raportu Gartner pt. „Magic Quadrant for Enterprise Wired and Wireless LAN" za rok 2025 r. lub równoważnym. Jako ranking równoważny Zamawiający uzna ranking klasyfikujący rozwią-zania enterprise przewodowych i bezprzewodowych sieci LAN, prowadzony i publikowany przez podmiot niezależny od producentów tych rozwiązań. Zamawiający wymaga, aby ranking taki był aktualizowany w okresach nie dłuższych niż 1 rok. Podstawą do sporzą-dzenia raportów muszą być badania polegające na sprawdzeniu jakości oferowanych usług i rozwiązań.

VIII.Odnowienie Licencji EDR dla Urzędu

Przedmiotem zamówienia jest odnowienie oprogramowania EDR dla min. 40 użytkowników (Check Point Harmony Endpoint Advanced lub rozwiązanie równoważne o parametrach nie gorszych niż w opisie poniżej).

Wymagania dla oprogramowania EDR są następujące:

Warunki ogólne:

- Wsparcie dla systemów

- Windows: 7/8/10/11
- Windows Server: 2008 R2, 2012 R2, 2016 2019 2022,
- Macos 10.14/10.15/11/12
- Linux Ubuntu, SLES, RHEL, Oracle Linux, Open Suse, CentOS
- Wsparcie dla 32- i 64-bitowej wersji systemu Windows tam, gdzie jest to dostępne.

Wymagania dodatkowe:

- Zarządzanie końcówkami musi się odbywać z systemu zarządzania posiadanego przez zamawiającego.
- Agent ma wbudowany system zabezpieczeń uniemożliwiający dokonanie deinstalacji przez użytkowania.

Funkcje systemu ochrony antywirusowej:

a) Po stronie klienta ochrona przeciwwirusowa chroni komputery przed wirusami, programami szpiegującymi i złośliwym oprogramowaniem.
b) Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
c) Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
d) GUI po stronie panel klienta zawiera takie informacje jak:
   – bieżący status klienta oraz skanowania zasobów klienta
   – data i godzina ostatniego skanowania dysku
   – listę infekcji (z dokładnymi informacjami dotyczącymi skanowanego pliku)
   – listę obiektów w kwarantannie
e) Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
f) Możliwość skanowania „na żądanie” pliku, katalogu lub wybranego napędu
g) Ręczna opcja aktualizacji sygnatur wirusów w dowolnej chwili
h) Możliwość tworzenia list wyjątków zawierający zbiory lub katalogi
i) Możliwość tworzenia whitelist z wyjątkami procesów
j) Mechanizm wykrywania ataków typu Ransomware, polegający na monitorowaniu zachowania się uruchomionych programów i operacji w przestrzeni dyskowej a także blokowaniu w przypadku nieprawidłowego ich zachowania wraz z przywracaniem zaszyfrowanych plików.
k) Wszystkie aktywności modułu przeciwwirusowego są logowane i przesyłane do centralnego systemu zarządzania.
l) System zabezpieczeń antibot wykorzystuje następujące technologie:
   – Identyfilacja adresów C&C
   – Identyfikacja wzorców komunikacyjnych (sygnatur)
m) Identyfikacja zachowania bota

Funkcje modułu zgodności:
Narzędzie zgodności weryfikuje zasady bezpieczeństwa utworzone przez administratora i

raportuje stan końcówki do serwera zarządzającego.

a) Narzędzie raportuje następujące stany zgodności:
   - Compliant
   - Warn
   - About to be restricted
   - Restricted
b) Narzędzie raportuje następujące stany komputera końcowego (Windows)
   - Wszystkie monitorowane funkcjonalności są zainstalowane i uruchomione na komputerze końcowym
   - Oprogramowanie EDR jest uruchomione, a silnik i bazy sygnatur są aktualne.
   - Na komputerze końcowym zainstalowane są wymagane dodatki Service Pack i aktualizacje systemu operacyjnego.
   - Na komputerze punktu końcowego są zainstalowane i uruchomione tylko autoryzowane programy.
   - Wymagane klucze i wartości rejestru są obecne
c) Polityki zgodności powinny obejmować:
   - weryfikację działania bloków oprogramowania klienta
   - weryfikację konfiguracji połączeń VPN
   - reguły działania polityk zgodności
   - dodatkowe reguły zgodności obiektów
   - reguły przywracania zgodności (z przepisami)
   - reguły zmian w rejestrach i uruchamiania zbiorów
   - reguły zgodności wersji oprogramowania systemowego
   - reguły zabronionego oprogramowania i plików

Wszystkie aktywności modułu zgodności są logowane i przesyłane do centralnego systemu zarządzania.

Funkcjonalność firewall:

a) Dla ochrony sieci definiuje się zestawy reguł takie jak:
   - Reguły firewall
   - Reguły kontroli aplikacji
   - Reguły dostępu do stref bezpieczeństwa
b) Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego
c) „reputacja plików" - zaawansowane metody analizy zbieranych informacji przez agenta o plikach powinny wystarczyć do określenia ich dyspozycji – czy są złośliwe, neutralne czy czyste
d) Reguły modułu firewall umożliwiają definiowanie osobnych reguł dla ruchu przychodzącego i wychodzącego
e) Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet
f) Możliwość stosowania zestawu reguł w zależności od strefy bezpieczeństwa np. sieć wewnętrzna, zewnętrzna, Wi-Fi, itp.

g) Możliwość blokowania ruchu internetowego na podstawie reputacji adresów URL. Lista reputacji URL jest na bieżąco dostarczana przez producenta oprogramowania
h) Możliwość definiowania własnych list (blacklist) adresów URL do blokowania.
i) Oprogramowanie umożliwia filtrowanie adresów URL w oparciu o kategorie i podkategorie
j) Możliwość blokowania ruchu LAN w zależności od podłączenia końcówki do sieci WLAN
k) Możliwość blokowania ruchu do sieci WLAN
l) Możliwość blokowania ruchu z aplikacji zainstalowanych na stacjach końcowych. Polityka umożliwia przypisanie reguły typu: allowed, blocked lub terminated

Funkcjonalność VPN

a) System powinien realizować funkcję bezpiecznych połączeń VPN typu tunel warstwy 3
b) Umożliwia dwuskładnikowe uwierzytelnianie użytkowników
c) Wspiera systemy Windows i Mac OS
d) Połączenie VPN musi być zgodne z systemami zapór sieciowych posiadanych przez zamawiającego
e) Proces uwierzytelniania VPN musi obsługiwać co najmniej:
   – Użytkownik/hasło
   – Certyfikat CAPI
   – Certyfikat P12
   – Token SecureID KeyFob
   – Token SecureID PinPad
   – Uwierzytelnianie challenge-response

Konsola zarządzania:

a) Konsola zarządzania jest osobnym systemem, przy pomocy którego odbywa się zarządzanie wszystkimi końcówkami.
b) Konsola umożliwia wgląd w ogólny stan bezpieczeństwa końcówek, aktywne alarmy bezpieczeństwa i bieżący status bezpieczeństwa
c) Główne funkcje konsoli bezpieczeństwa to:
   – Zarządzanie politykami bezpieczeństwa
   – Zarządzanie użytkownikami i stacjami końcowymi
   – Funkcje raportowania
d) Konsola umożliwia ręczne lub automatyczną instalację agentów na końcówkach
e) Moduł zarządzania musi być obsługiwany za pomocą konsoli użytkownika, która jest dostarczona w postaci dedykowanej graficznej konsoli działającej na osobnym komputerze Windows.
f) Komunikacja klienta końcowego z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
g) System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez REST API, do którego producent udostępnia dokumentację.
h) Konsola zarządzania posiada mechanizm instalacji zdalnej agenta na stacjach roboczych w dowolnej konfiguracji składającej się z poszczególnych funkcji agenta
i) Konsola umożliwia podział zarządzanych stacji roboczych na grupy, którym przypisuje się ich własną politykę.
j) Konsola umożliwia przypisanie osobnej polityki dla każdej końcówki z osobna.

k) Konsola umożliwia pełną konfigurację połączenia VPN na etapie definicji agenta (nazwa, adres IP wraz z metodami uwierzytelniania)
l) Konsola zarządzania umożliwia w dowolnym momencie wykonanie następnych operacji:
   – Skan plików i folderów
   – Aktualizacja bazy sygnatur
   – Odblokowanie zbiorów z kwarantanny
   – Objęcie zbiorów kwarantanną
   – Izolacja danego komputera
   – Odblokowanie komputera ze stanu izolacji
   – Shutdown i restart końcówki
   – Odinstalowanie agenta
   – Naprawa agenta
   – Przesłania logów agenta
   – Wykonanie komendy zdalnej
m) Konsola posiada możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie konsola zarządzania współpracuje z serwerem Active Directory w celu pozyskania informacji o grupach, użytkownikach i komputerach