

IR.271.5.10.2025

Załącznik do SWZ nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

Część nr 1: Urządzenia komputerowe

Zamawiający w opisie przedmiotu zamówienia wskazuje wyłącznie jako przykładowy wzór konkretnego producenta. Zamawiający dopuszcza zastosowanie sprzętu i oprogramowania równoważnego, poprzez który należy rozumieć sprzęt i oferowane oprogramowanie o parametrach nie gorszych od opisanych jako wymagane, umożliwiające wykorzystanie urządzeń, w takim samym zakresie i stopniu skomplikowania, co sprzęt i oprogramowanie określone w opisie przedmiotu zamówienia. Uwaga nie ma zastosowania do systemu operacyjnego serwera, w przypadku którego Zamawiający wskazuje konkretne rozwiązanie należące do konkretnego producenta oprogramowania.

Macierz dyskowa z serwerem i oprogramowaniem

Przedmiotem zamówienia jest dostawa i wdrożenie macierzy dyskowej z serwerem wraz z systemem backupowym na co najmniej 5 wirtualnych środowisk ze wsparciem 12 miesięcy.

Element konfiguracji/cecha/funkcjonalność	Wymagania minimalne macierzy dyskowej
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19", o wysokość maksymalnie 2U z możliwością instalacji min. 12 dysków 3.5"
Przestrzeń dyskowa	Zainstalowane: 6x dysk SAS o pojemności min. 16TB, Hot-Plug
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 dysków twardych.
Obsługa dysków	Macierz musi mieć możliwość obsługi dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5" jak również 3,5".
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.

Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania baterijnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać, co najmniej 8 portów 12Gb SAS (4 porty na kontroler)
Kable/wkładki	2x kabel 12Gb HD Mini-SAS/HD Mini-SAS min. 2m
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą

	<p>wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.</p> <p>Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>
Wewnętrzne kopie pełne	<p>Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>
Migracja danych w obrębie macierzy	<p>Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.</p>
Podłączanie zewnętrznych systemów operacyjnych	<p>Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).</p> <p>Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix.</p> <p>Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.</p>
Redundancja	<p>Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.</p> <p>Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.</p> <p>Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.</p> <p>Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.</p>
Dodatkowe wymagania	<p>Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez</p>

	<p>dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.</p> <p>Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.</p>
Standardy bezpieczeństwa	<p>Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające spełnienie powyższych zaleceń.</p>
Inne	<p>Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.</p> <p>Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.</p> <p>Deklaracja zgodności CE.</p>
Warunki gwarancji	<p>Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat.</p> <p>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.</p> <p>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.</p> <p>Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</p> <p>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.</p> <p>Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</p> <p>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.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p> <p>Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:</p> <ul style="list-style-type: none"> • 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

	<p>problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.</p> <ul style="list-style-type: none"> • Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. • Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. • Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaze dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. <p>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.</p>
--	--

Element konfiguracji/cecha /funkcjonalność	Wymagania minimalne serwera
Obudowa	<ul style="list-style-type: none"> • Obudowa Rack o wysokości maksymalnie 1U • Minimalnie 8 wnęk na dyski 2.5" • Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej • 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 do dwóch procesorów. • Obsługa procesorów 32 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	<ul style="list-style-type: none"> • Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.

Procesor	<ul style="list-style-type: none"> Zainstalowany jeden procesor min. 8-rdzeniowy, min. 2.6GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 169 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	<ul style="list-style-type: none"> 64GB DDR5 RDIMM 5600MT/s,
Kontroler RAID	<ul style="list-style-type: none"> Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10
Dyski twarde	<ul style="list-style-type: none"> Zainstalowane: <ul style="list-style-type: none"> 2x dysk SSD SATA o pojemności min. 480GB, Hot-Plug Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB z możliwością konfiguracji RAID 1.
Gniazda PCI	<ul style="list-style-type: none"> Jeden slot PCIe LP
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Czteroportowa karta 12Gb SAS HBA
Wbudowane porty	<ul style="list-style-type: none"> 4 porty USB w tym: <ul style="list-style-type: none"> 1 port USB 3.0 z tyłu obudowy, 1 port micro USB z przodu obudowy 2 port VGA z czego jeden z przodu obudowy Możliwość rozbudowy o port RS232
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. 700W klasy Titanium
Elementy montażowe	<ul style="list-style-type: none"> Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
System operacyjny/dodatkové oprogramowanie	<ul style="list-style-type: none"> Windows Server 2025 Standard Nośnik CD/DVD umożliwiający downgrade do wersji Windows Server 2022 Standard
Bezpieczeństwo	<ul style="list-style-type: none"> Zatrzaśk górnej pokrywy 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

	<ul style="list-style-type: none"> • 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	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające:</p> <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, 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 <ul style="list-style-type: none"> ○ Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych,

	<p>HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON</p> <ul style="list-style-type: none"> • Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. • Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera • Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej 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 lub WIFI. <p>Możliwość rozszerzenia funkcjonalności karty o:</p> <ul style="list-style-type: none"> • 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 • kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania • Automatyczne odświeżanie certyfikatów SSL • możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej • możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień • możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera • możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer • możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe • monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	<p>Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</p> <ul style="list-style-type: none"> • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF

- Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
- Grupowanie urządzeń w oparciu o kryteria użytkownika
- Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
- 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
- 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 modułowych oraz przełączników sieciowych w oparciu o profile
- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.

	<ul style="list-style-type: none"> • 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.
Oprogramowanie do monitorowania	<p>Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wirtualizacji VMware. 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 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: <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

	<p>informacja o anomaliach.</p> <ul style="list-style-type: none"> • Monitoring parametrów pamięci masowych z informacją o minimum: <ul style="list-style-type: none"> ○ Opóźnień ○ 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: <ul style="list-style-type: none"> ○ 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 <ul style="list-style-type: none"> ○ 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 <ul style="list-style-type: none"> ○ Możliwość generowania raportów dla serwerów
--	---

	<p>zawierających informację o:</p> <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 <ul style="list-style-type: none"> • 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.
--	--

	<ul style="list-style-type: none"> 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. 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 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

	<p>zakończenia diagnostyki.</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ 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. • 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.
--	--

Wymagania systemu backupowego:

Funkcjonalność wykonywania kopii zapasowych z urządzeń typu: serwery fizyczne, maszyny wirtualne, stacje końcowe). Subskrypcja powinna zawierać produkcyjne wsparcie 24/7. zapewnia centralne backupy, odtwarzanie, raportowanie i monitoring z poziomu jednej konsoli. W zakresie licencji wymaga ochrony co najmniej 5 środowisk z możliwością rozbudowy. Licencja powinna być uniwersalna i przenośna między fizycznymi, wirtualnymi i chmurowymi środowiskami.

W ramach prac wdrożeniowych przeprowadzone zostaną następujące czynności:

- Wdrożenie zestawu macierzy dyskowej z serwerem do wykonywania kopii bezpieczeństwa
 - Instalacja fizyczna oraz podłączenie we wskazanej lokalizacji
 - Aktualizacja oprogramowania systemowego urządzenia, jeśli wymagane
 - Inicjalizacja i konfiguracja macierzy i serwera
 - Integracja macierzy i serwera z systemem backupowym
 - Konfiguracja polityk backupowych na 2 fizycznych środowiskach serwerowych
 - Weryfikacja poprawności wykonania backupów wraz z naprawą potencjalnych usterek.
 - Weryfikacja poprawności odtwarzania danych z backupu wraz z naprawą potencjalnych usterek.
- Dokumentacja powdrożeniowa
- Szkolenie w zakresie obsługi i konfiguracji dostarczonego sprzętu pracownika wskazanego przez Zamawiającego.
- Odbiór prac przez Zamawiającego

Konfiguracji urządzeń dokona inżynier posiadający doświadczenie do wykonywania prac. Na potwierdzenie wykonania konfiguracji zostaną wykonane testy potwierdzające zgodność dostarczonych komponentów z wymaganiami Zamawiającego (Opisem Przedmiotu Zamówienia).

Oprogramowanie do zarządzania infrastrukturą IT

Przedłużenie posiadanej licencji ITManager o 12 miesięcy pozwalająca na obsługę 70 stanowisk roboczych według poniższych funkcjonalności.

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, Agenta/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 przełączenia 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:

- 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.

Zarządzanie zasobami oraz użytkownikami

Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami.

Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu.

Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość.

Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np.

powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów.

Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiające powiązania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem.

Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) w **strukturze drzewiastej** wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.

Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów.

Oprogramowanie musi umożliwiać import danych z zewnętrznego pliku CSV zawierającego informacje inwentaryzacyjne z nowo zakupionych urządzeń w zakresie: numer faktury, numer seryjny, model, nazwa, data zakupu.

Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV.

Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej.

Oprogramowanie musi zawierać wbudowany kreator wydruków w zakresie protokołów przekazania, zwrotu, likwidacji wraz z możliwością utworzenia dowolnego typu dokumentu

Oprogramowanie musi umożliwiać export ww. protokołów w formacie PDF

Oprogramowanie musi umożliwiać obsługę kodów kreskowych oraz QR w obrębie ww. kreatora wydruków

Oprogramowanie musi umożliwiać użycie w kreatorze wydruków własnego logotypu organizacji

Oprogramowanie musi umożliwiać użycie w kreatorze wydruków dowolnego atrybutu zasobu

Oprogramowanie musi umożliwiać przypisanie dowolnej firmy serwisowej z bazy organizacji do zasobu

Oprogramowanie musi umożliwiać przypisanie załącznika do zasobu

Oprogramowanie musi umożliwiać pogląd wszystkich zgłoszeń serwisowych dotyczących danego zasobu

Oprogramowanie musi umożliwiać podgląd zasobów (przypisanych do danego pracownika) z poziomu jego portalu użytkownika końcowego

Oprogramowanie musi umożliwiać zarządzanie cyklem życia zasobu

Oprogramowanie musi umożliwiać tworzenie niestandardowych reguł biznesowych dla zarządzania zasobami

Oprogramowanie musi umożliwiać seryjne dodawanie zasobów

Oprogramowanie musi umożliwiać automatyczne nadawanie numerów inwentaryzacyjnych dla zasobów

Oprogramowanie musi udostępniać kreator raportów dla zasobów

Oprogramowanie musi udostępniać możliwość kopiowania widoku dla określonego typu(ów)

zasobu z innego typ zasobu

Oprogramowanie musi udostępniać możliwość kopiowania formularz dla określonego typu(ów) zasobu z innego typ zasobu

Oprogramowanie musi umożliwiać ewidencję magazynów

Oprogramowanie musi umożliwiać ewidencję lokalizacji magazynowych

Oprogramowanie musi umożliwiać ewidencję produktów magazynowych

Oprogramowanie musi udostępniać informację o stanie magazynowym(ilościowo)

Oprogramowanie musi umożliwiać generowanie dokumentów PZ/PW/RW/MM

Oprogramowanie musi umożliwiać przyjęcie zasobów ewidencjonowanych i eksploatacyjnych na magazyn

Oprogramowanie musi umożliwiać wydawanie zasobów ewidencjonowanych i eksploatacyjnych z magazynu

Oprogramowanie musi umożliwiać zwrot zasobów na magazyn

Oprogramowanie musi umożliwiać zmianę szablonów dokumentów PZ/PW/RW/MM

Oprogramowanie musi umożliwiać wyszukiwanie dokumentów po dowolnym atrybucie

Oprogramowanie musi umożliwiać zarządzanie organizacjami/typami organizacji (np. klient, podwykonawca)

Oprogramowanie musi umożliwiać dowolne przypisanie osoby do organizacji

Oprogramowanie musi umożliwiać tworzenia dynamicznych grup użytkowników

Oprogramowanie musi umożliwiać zarządzanie kontaktami osób/organizacji

Oprogramowanie musi umożliwiać zarządzanie nieobecnościami użytkowników

Oprogramowanie musi umożliwiać zarządzanie uprawnieniami i poziomami dostępu do danych w zakresie zarządzania zasobami

Oprogramowanie musi umożliwiać automatyczne pobieranie danych rejestrowych kontrahentów z bazy GUS

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 dystrybucji zadań 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

Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.

Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań 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 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.

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 wznawiać 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).

ServiceDesk – Zarządzanie zgłoszeniami

Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności:

- Zarządzanie problemem
- Zarządzanie incydem
- Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy)
- Zarządzanie umowami serwisowymi
- Definicje poziomów SLA (reakcja, naprawa, reklamacja)

Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora.

Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW na urządzeniach mobilnych poprzez responsywny interfejs użytkownika.

Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski).

Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień.

Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu.

Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP.

Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmu SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.

Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu.

Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia.

Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.

Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w

zależności od zalogowanego użytkownika.

Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika.

Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego.

Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu.

Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników.

Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika.

Oprogramowanie musi umożliwiać tworzenie szablonów zadań.

Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna.

Oprogramowanie musi umożliwiać przysyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu.

Oprogramowanie musi umożliwiać edycję szablonów powiadomień email.

Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii.

Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika.

Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia.

Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika.

Rozwiązania w bazie wiedzy muszą posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT. Panel www użytkownika musi zawierać wyszukiwarkę tematów wg słów kluczowych oraz wewnętrznej treści.

Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników.

Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefoniczna informacja o awarii komputera).

Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika).

Oprogramowanie musi umożliwiać obsługę tzw. Linii wsparcia poprzez samodzielne tworzenie nowych linii wraz z przypisywaniem do nich dowolnej ilości kont operatorów HelpDesk. Zgłoszenie serwisowe musi mieć możliwość przekazania do dowolnej linii wsparcia lub dedykowanego operatora HelpDesk. Linia wsparcia musi mieć możliwość przypisania powiązanych z nią kategorii zgłoszeń.

Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.

Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika.

Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). lub z zakupionym sprzętem.

Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis

przekazania zgłoszenia do serwisu zewnętrznego.

Oprogramowanie musi umożliwiać przysyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem.

Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia (w komentarzach) korespondencji

mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem.

Oprogramowanie musi posiadać dedykowane panele WWW w zależności od aktywnie zalogowanego użytkownika końcowego (panel dla użytkownika tj. zgłaszanie incydentów, panel dla operatora serwisowego – obsługa zgłoszeń, panel dla managera HelpDesk – analiza graficzna oraz tabelaryczna pracy operatorów HelpDesk).

Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia).

Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia.

Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc)

Oprogramowanie musi umożliwiać tworzenie reguł w celu automatyzacji obsługi zgłoszeń. Reguły muszą uruchamiać się w odpowiedzi na określone zdarzenia w systemie i wykonywać akcje w zależności od spełnionych warunków. W zakresie reguł ServiceDesk musi realizować m.in. następujące przypadki użycia:

- Zmiana statusu po przejęciu zgłoszenia przez opiekuna.
- Przejmowanie zadań po przejęciu zgłoszenia przez opiekuna.
- Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia.
- Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika.
- Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika.
- Zamykanie zgłoszenia po upływie czasu reklamacji.
- Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów.
- Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza.
- Walidacja zamkniętych zadań w zamykanym zgłoszeniu.
- Systemowe potwierdzanie realizacji zgłoszenia.
- Wysyłanie dodatkowych powiadomień cyklicznych ze zgłoszeniami, np. zgłoszenia wymagające reakcji, zgłoszenia do realizacji lub zgłoszenia wstrzymane/wznowione.

Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń.

Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników.

Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email.

Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).

Oprogramowanie musi umożliwiać definiowanie własnych widoków oraz zestawień dla każdego zalogowanego użytkownika

Oprogramowanie musi umożliwiać zdefiniowanie własnej macierzy priorytetów na podstawie pilności oraz wpływu zgłoszenia

Oprogramowanie musi umożliwiać zamodelowanie trybu pracy inżynierów (opiekunów zgłoszeń)

Oprogramowanie musi umożliwiać informowanie użytkowników o nowych zdarzeniach systemowych za pomocą notyfikacji (dymku) podczas pracy z systemem

Oprogramowanie musi umożliwiać tworzenie obiegu procesu decyzyjnego dla wniosków o uprawnienia lub elementy konfiguracji w oparciu o bazę C MDB

Oprogramowanie musi umożliwiać zaprojektowanie dowolnego formularza do wprowadzania danych z wykorzystaniem własnych atrybutów (wraz ze zmianą układu/położenia atrybutów w projektowanym widoku)

Oprogramowanie musi umożliwiać definicję czasów SLA w oparciu o matrycę priorytetów, statusy, kategorie lub dowolne warunki i atrybuty zgłoszenia

Oprogramowanie musi umożliwiać dodanie Akceptacji do już istniejącego zgłoszenia

Oprogramowanie musi umożliwiać definiowanie własnych reguł zarządzania w oparciu o warunki i akcje dla Prawdy i Fałszu (zdarzenie -> warunek -> akcja)

Oprogramowanie musi umożliwiać tworzenie wielu zgłoszeń poprzez wybór kilku użytkowników w zgłoszeniu

Oprogramowanie musi umożliwiać tworzenie słowników wartości dla atrybutów w oparciu o strukturę płaską lub drzewiastą

Oprogramowanie musi umożliwiać tworzenie atrybutów zależnych poprzez określone warunki widoczności

Oprogramowanie musi umożliwiać definiowanie formularzy zamykających zgłoszenie oraz zatwierdzające zmiany w zgłoszeniu

Oprogramowanie musi umożliwiać definiowanie reguł biznesowych za pomocą graficznego/blokowego kreatora.

Oprogramowanie musi umożliwiać definiowanie obiegu za pomocą graficznego/blokowego kreatora.

Oprogramowanie musi umożliwiać tworzenie niestandardowych raportów za pomocą kreatora.

Oprogramowanie musi umożliwiać definiowanie poziomu dostępu do zgłoszeń dla dynamicznych grup użytkowników.

Oprogramowanie musi umożliwiać definiowanie formularzy dla zgłoszeń w danej kategorii za pomocą kreatora Drag&Drop z możliwością określenia układu kolumn.

Oprogramowanie musi umożliwiać tworzenie dowolnej liczby Dashboard-ów dla użytkownika za pomocą kreatora Drag&Drop.

Oprogramowanie musi umożliwiać zmianę układu szczegółów zgłoszenia za pomocą kreatora Drag&Drop.

Oprogramowanie musi umożliwiać udostępniania ogłoszeń w formie Widget-u oraz okienka modalnego z wymaganym potwierdzeniem dla użytkownika.

Oprogramowanie musi umożliwiać zaprojektowanie dowolnego szablonu protokołu zgłoszenia.

Oprogramowanie musi udostępniać matrycę(wpływ/pilność) dla obliczania priorytetu zgłoszeń.

Oprogramowanie musi umożliwiać zmianę koloru dla statusu/priorytetu/wpływu/pilności zgłoszenia prezentowanego na liście zgłoszeń.

Oprogramowanie musi umożliwiać definiowanie dowolnych kolejek zgłoszeń.

Oprogramowanie musi umożliwiać rejestrację nieobecności administratorów z możliwością wybrania zastępstwa.

Monitoring sieci LAN

Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony

Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować o błędach takich jak brak papieru, zacięcie papieru.

Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.

Oprogramowanie musi umożliwiać z zdaną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.

Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.

Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.

Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.

Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.

System wewnętrznego komunikatora dla użytkowników

Oprogramowanie musi zawierać wewnętrzny komunikator pracujący w sieci LAN, integrujący się z usługą katalogową w zakresie kont użytkowników (dane osobowe, avatar), jednostek organizacyjnych.

Oprogramowanie w zakresie modułu komunikatora dla użytkowników musi współpracować z serwerem MSSQL Server 2008R2-2019 lub PostgreSQL

Oprogramowanie komunikatora musi umożliwiać automatyczne logowanie użytkowników pochodzących z usługi katalogowej.

Oprogramowanie komunikatora musi umożliwiać konwersację grupową oraz prywatną pomiędzy użytkownikami

Oprogramowanie komunikatora musi umożliwiać wysyłanie wiadomości powitalnych; komunikatów grupowych z raportowaniem doręczenia oraz odczytania.

Oprogramowanie komunikatora musi umożliwiać generowanie raportów doręczenia/odczytania wiadomości wymagających potwierdzenia.

Oprogramowanie komunikatora musi umożliwiać określenie maksymalnego rozmiaru transferowanego pliku (przez administratora).

Oprogramowanie komunikatora musi umożliwiać wysyłanie powiadomień e-mail o utworzeniu/modyfikacji użytkowników, którzy nie pochodzą z usługi katalogowej.

Oprogramowanie komunikatora musi umożliwiać automatyczną aktualizację wg. zadanej konfiguracji danych synchronizowanych (ze szczególnym uwzględnieniem danych o użytkownikach, jednostkach organizacyjnych z usługi katalogowej).

Oprogramowanie komunikatora musi umożliwiać archiwizację starych rozmów między użytkownikami.

Oprogramowanie komunikatora musi umożliwiać administratorowi wyłączenie globalnie możliwości zamknięcia/wylogowanie/zapisywanie poświadczeń dla klientów końcowych.

Oprogramowanie komunikatora musi umożliwiać administratorowi bezpieczeństwa wgląd do rozmów pracowników, wyłączenie wybranych funkcjonalności dla klienta końcowego (np. transferu plików, konferencji audio-video).

Oprogramowanie komunikatora musi umożliwiać wymianę plików pomiędzy zalogowanymi

użytkownikami

Oprogramowanie komunikatora musi umożliwiać nawiązanie sesji audio oraz wideo pomiędzy zalogowanymi użytkownikami wraz z obsługą konferencji grupowych.

Wymagania formalne:

Support dla 70 posiadanych licencji oprogramowania ITManager oraz 1 dostępu administracyjnego musi zawierać 12 miesięczny support producenta, liczony od daty zakończenia obecnie posiadanego wsparcia (wygasającego w dniu 16.11.2025r.).

Obsługa serwisowa w zakresie obsługi błędów realizowana ma być z czasem reakcji 16 godzin roboczych oraz czasem naprawy 80 godzin roboczych. W ramach supportu wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.

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.

Oprogramowanie antywirusowe

Przedmiotem zamówienia jest przedłużenie posiadanej licencji na oprogramowanie antywirusowe Bitdefender GravityZone Business Security Premium (Elite) dla 65 urządzeń na okres 12 miesięcy.

Wymagania dotyczące licencji

- **Zamówienie obejmuje przedłużenie istniejącej licencji Bitdefender [nazwa posiadanej wersji, np. GravityZone Business Security].**
- **Licencja powinna być zgodna z już posiadaną infrastrukturą oraz zapewniać ciągłość ochrony bez konieczności reinstalacji oprogramowania.**
- **Wymagane wsparcie techniczne producenta przez cały okres trwania licencji.**
- **Przedłużenie powinno obejmować pełen zakres funkcjonalności obecnie posiadanego pakietu.**

Warunki dostawy i aktywacji licencji

- **Licencja musi być dostarczona w formie elektronicznej, z kluczami aktywacyjnymi oraz instrukcją aktywacji.**
- **Wykonawca zobowiązany jest do wsparcia w zakresie aktywacji i konfiguracji (jeśli wymagane).**

Wymagania oprogramowania antywirusowego:

Ochrony środowisk wirtualnych (SVE)

1. **Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej**
2. **Maszyna wirtualna pełniąca rolę silnika skanującego może być pobrana w formacie:**
 - a) **OVA**

- b) XVA
- c) VHD
- d) VHDX
- e) VMDK

Środowiska wspierane:

- VMware vSphere and vCenter Server:
 - version 6.5
 - version 6.7, including update 1, update 2a and update 3
 - version 7.0, including update 1, update 2, update 2b, update 2c and update 2d
 - version 8.0, including update 1, update 2
- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix Xen Hypervisor: 7.1 (with the XS71ECU2060 hotfix), 8.2.
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (including Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1

- Nutanix Prism with AOS 5.6, 5.5, 5.20 LTS, 5.18 STS, 5.15 LTS, 5.11, 5.10 (Enterprise Edition)
- Nutanix Prism with AHV 20170830.115, 20170830.301, 20170830.395 and 20190916.294 (Community Edition)

Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Interfejs oraz pomoc techniczna świadczona w języku polskim.
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi.
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
5. Wbudowana technologia do ochrony przed rootkitami.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. Możliwość ustawienia zadania skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Ochrona krytycznych kluczy rejestru przed ich wykorzystaniem lub nieautoryzowanym dostępem do nich.
13. Możliwość dodawania wykluczeń na podstawie:
 - a) Plik
 - b) Folder
 - c) Rozszerzenie
 - d) Proces
 - e) Hash pliku



- f) Hash certyfikatu
 - g) Nazwa zagrożenia
 - h) Wiersz poleceń
 - i) IP/maska
14. Skanowanie poczty opartej o protokoły POP3 i SMTP w czasie rzeczywistym.
 15. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie w przeglądarce.
 16. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
 17. Wsparcie przeglądarek Internet Explorer 8+, Mozilla Firefox 30+, Google Chrome 34+, Safari 4+, Microsoft Edge 20+ i Opera 21+ bez konieczności zmian w konfiguracji.
 18. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH.
 19. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
 20. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
 21. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia, kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i godziny.
 22. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
 23. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
 24. Administrator musi mieć możliwość ukrycia ikony oprogramowania w obszarze powiadomień systemu Windows.
 25. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na punkcie końcowym Windows i macOS.



26. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
27. Oprogramowanie klienckie posiada wbudowaną funkcję do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
28. System musi umożliwiać kontrolę dostępu do urządzeń na podstawie interfejsów, do których zostały one podłączone.
29. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej na podstawie ich wykrycia lub wpisanych ręcznie ID urządzenia lub ID produktu.
30. Funkcja blokowania informacji wysyłanych przez HTTP lub SMTP jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.).
31. Funkcja blokowania wysyłanych informacji konfigurowana zdalnie przez administratora.
32. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
33. Wbudowany IDS.
34. Możliwość wykorzystania funkcji skanowania lokalnego lub hybrydowego ze sprawdzaniem reputacji plików w chmurze.
35. Możliwość tworzenia list sieci zaufanych.
36. Możliwość dezaktywacji funkcji zapory sieciowej.
37. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
38. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa).
39. Komunikacja między konsolą zarządzającą, a punktami końcowymi jest szyfrowana.
40. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z



nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:

- a) Możliwość wymuszenia funkcji DEP systemu Windows.
- b) Możliwość wymuszenia relokacji modułów (ASLR) dla Windows.

41. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak:

- Pierwszy dostęp.
- Dostęp do poświadczeń.
- Wykrycie.
- Crimeware.
- Ruch boczny.

42. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików, a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji. Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznie.

Formaty plików jakie mogą być odzyskane:

3fr, ai, arw, bay, cdr, cer, cr2, crt, crw, dcr, der, dll, dng, doc, docm, docx, dwg, dxf, dxg, eps, erf, exe, indd, jpe, jpeg, jpg, mdf, mef, mrw, nef, nrw, odb, odc, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, pdf, pef, pem, pfx, ppt, pptm, pptx, psd, pst, ptx, png, r3d, raf, rtf, rw2, rwl, sr2, srf, srw, wb2, wpd, wps, x3f, xlk, xls, xlsb, xlsx, msg, py, ini, xml, msi, cab, tsf, dgn, log, gif, csv, avi, mov, mp4

43. System musi wykrywać podatne sterowniki zainstalowane na punkcie końcowym z Windows i Linux.

44. Agent i usługi oprogramowania antywirusowego zainstalowanego na punkcie końcowym muszą być chronione przed próbami manipulacji i naruszenia ich integralności w systemie Windows.

45. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows.
46. System musi umożliwiać skanowanie oprogramowania układowego UEFI.
47. System umożliwia przechwytywanie TLS handshake pozwalając na skanowanie ruchu sieciowego bez konieczności deszyfracji.

Stacje robocze i serwery

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.
4. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
5. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.
6. Produkt i zawartość zabezpieczeń powinny być aktualizowane nie rzadziej niż raz na godzinę.
7. Oprogramowanie posiada możliwość raportowania zdarzeń informacyjnych.
8. Oprogramowanie musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
9. Oprogramowanie musi posiadać możliwość skanowania jedynie nowych i zmienionych plików.
10. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji na systemach Windows po doinstalowaniu odpowiedniego modułu. Zmiana ustawień zabezpieczona jest hasłem.
11. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji „O programie”, możliwość wyświetlenia danych do pomocy technicznej tj: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony.



12. Dla maszyn z systemem Linux możliwość wskazania katalogów, które mogą być chronione w czasie rzeczywistym.

Ochrona Exchange

1. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.
2. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w ciągu określonego czasu.
3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz niemożliwych do przeskanowania.
4. Możliwość skanowania w poszukiwaniu potencjalnie niechcianych aplikacji (PUA).
5. Możliwość skanowania malware wewnątrz archiwów.
6. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen.
7. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.
8. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy.
9. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi.
10. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowanie maila do konkretnej skrzynki pocztowej.
11. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością.
12. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila,



usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.

Konsola zdalnej administracji

1. System musi umożliwiać centralne zarządzanie i konfigurację ochrony wspieranych stacji roboczych i serwerów.
2. Możliwość integracji wielu domen Active Directory.
3. Możliwość uruchomienia zdalnego skanowania wybranych punktów końcowych.
4. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony punktu końcowego (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania na żądanie, zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
5. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi.
6. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, systemu operacyjnego.
7. Możliwość centralnej aktualizacji punktów końcowych z serwera w sieci lokalnej lub z Internetu.
8. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
9. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
10. Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) oraz wyeksportowanie ich do formatu: pdf i csv. Również zbiorczo w formie archiwum zip.
11. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie.



12. Możliwość generowania raportu co godzinę.
13. Pierwsza aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
14. Możliwość dodania etykiety do stacji roboczej.
15. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
16. Możliwość przechowywania kwarantanny maksymalnie 180 dni.
17. Możliwość definiowania, czy pliki z kwarantanny mają być przesyłane do producenta i co ile godzin ma się ta czynność odbywać.
18. Po aktualizacji zawartości bezpieczeństwa opcja automatycznego przeskanowania kwarantanny.
19. Wsparcie techniczne mailowe i telefoniczne w j. polskim od poniedziałku do piątku w godzinach 8:00-16:00. W pozostałych godzinach możliwość bezpośredniego kontaktu z producentem (24/7) w j. angielskim.
20. Po integracji z lokalnym Active Directory możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
21. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji. Określenie lokalizacji na podstawie:
 - Zakres adresów IP/IP.
 - Adres bramy.
 - Adres serwera WINS.
 - Adres serwera DNS.
 - Połączenie DHCP sufiksów DNS.
 - Punkt końcowy może rozwiązać hosta.
 - Typ sieci.
 - Nazwa hosta.
22. Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238.

23. Możliwość naprawy instalacji agenta z poziomu konsoli.
24. Możliwość utworzenia reguły, która będzie usuwała punkty końcowe z konsoli zarządzającej, jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn, które automatycznie będą usuwane oraz na określenie godziny, o której te maszyny będą usuwane.
25. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
26. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
27. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux lub MacOS
28. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
29. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS.
30. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M oraz osobnego pakietu dla systemów Windows z Intel x86 oraz oddzielnego dla architektury ARM.
31. System umożliwia pobieranie plików poddanych kwarantannie z poziomu centralnej konsoli administracyjnej.
32. Możliwość wygenerowania i zapisania logów na stacji roboczej z poziomu konsoli zarządzającej.
33. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
34. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Przypisywanie musi odbywać się ręcznie lub automatycznie. Musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.
35. Ochrona proaktywna oparta o maszynowe uczenie, która działa w fazie poprzedzającej wykonanie. Ochrona ta musi wykrywać zagrożenia takie jak:
 - a) Ukierunkowane ataki.



- b) Podejrzane pliki i ruch w sieci.
 - c) Exploity.
 - d) Ransomware.
 - e) Grayware.
36. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego.
37. Moduł ochrony proaktywnej musi działać w trybach, które administrator może dowolnie zmieniać na:
- a) Tolerancyjny.
 - b) Normalny.
 - c) Agresywny.
38. Zintegrowany sandbox po stronie producenta, który pozwala na analizę pliku:
- a) Plik może zostać wysłany automatycznie ze stacji roboczej, jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora.
 - b) Możliwość ręcznego przesłania archiwum zabezpieczonego hasłem.
 - c) Możliwość ręcznego przesłania adresu URL.
 - d) W przypadku ręcznego przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.
39. Wbudowany sandbox musi działać w trybie monitorowania i blokowania.
40. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja, przeniesienie do kwarantanny lub tylko raportowanie.
41. Wbudowany sandbox musi oferować opcję wstępnego filtrowania plików z kategorii aplikacje, dokumenty, skrypty, archiwa, maile zapisane do pliku pod kątem podejrzanego zachowania.



42. Wbudowany sandbox musi posiadać opcję, która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.
43. Minimalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 1KB.
44. Maksymalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 50MB.
45. Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie interaktywnego wykresu i chronologicznej linii zdarzeń oraz daje możliwość:
 - a) Filtrowania zdarzeń.
 - b) Zakończenia procesów.
 - c) Dodania procesów do czarnej listy.
 - d) Dodania procesów do białej listy.
 - e) Izolacji hosta.
 - f) Przesłania pliku do Sandbox.
 - g) Sprawdzenia informacji o pliku w Google.
 - h) Sprawdzenia informacji o pliku w VirusTotal.
46. Możliwość szybkiego podglądu incydentów za pomocą modyfikowalnych widoków list lub widoku domyślnego.
47. Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie.
48. System umożliwia blokowanie na podstawie utworzonych reguł czarnej listy przy pomocy kategorii:
 - a) Hash MD5 lub SHA256.
 - b) Pełna ścieżka do aplikacji.
 - c) Reguła połączenia.



49. Możliwość importu reguł czarnej listy dla hash, ścieżek do aplikacji oraz reguł połączeń z pliku CSV.
50. System musi oferować szeroki zakres filtrowania dodanych reguł blokowania minimum po nazwie pliku, hash pliku, typu hash, ścieżce, protokole porcie/zakresie portów, daty dodania.
51. Zdarzenia z modułów mogą być przesyłane za pośrednictwem Syslog (JSON, CEF).
52. Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym.
53. Możliwość aktualizacji serwera administracyjnego bez potrzeby jego ponownej instalacji.
54. Możliwość określenia własnego serwera NTP.
55. Integracja z vCenter Server.
56. Integracja z Xen Server.
57. Integracja z nutanix Prism Element.
58. Integracja z Azure.
59. Możliwość przechowywania plików poddanych kwarantannie na scentralizowanym udziale.
60. System umożliwia zezwolenie na dostęp do konsoli zarządzającej dla użytkowników Active Directory z grupy Security Groups.
61. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:
 - a) Pakiety
 - b) Konta
 - c) Sieć
 - d) Kwarantanna
 - e) Raporty Polityki
62. Funkcja kontroli aplikacji, która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów. Może działać w trybie testowym lub produkcyjnym.



Pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat.

Wspierane systemy operacyjne

System Operacyjny Windows:

Systemy Operacyjne Komputerów

- Windows 11 October 2024 Update (24H2)
- Windows 11 October 2023 Update (23H2)
- Windows 10 November 2022 Update (22H2)
- Windows 11 September 2022 Update (22H2)
- Windows 11 (initial release)
- Windows 10 November 2021 Update (21H2)
- Windows 10 May 2021 Update (21H1)
- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 May 2019 Update (19H1)
- Windows 10 October 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10 (initial release)
- Windows 8.1
- Windows 8
- Windows 7 SP1

Windows Tablet oraz systemy wbudowane

Windows 10 IoT Enterprise



Windows Embedded 8.1 Industry

Windows Embedded 8 Standard

Windows Embedded Standard 7

Windows Embedded Compact 7

Windows Embedded POSReady 7

Windows Embedded Enterprise 7

Systemy operacyjne serwera

Windows Server 2025 64x

Windows Server 2022 Core

Windows Server 2022

Windows Server 2019 Core

Windows Server 2019

Windows Server 2016

Windows Server 2016 Core

Windows Server 2012 R2

Windows Server 2012

Windows Small Business Server (SBS) 2011

Windows Server 2008 R2

Systemy Operacyjne Linux i wersja kernel

Oparte o RPM

RHEL 7.x - 3.10.0 (build 957) 64-bit

RHEL 8.x - 4.18.0 64-bit

RHEL 9.x - 5.14.0 64-bit

Oracle Linux 7.x (UEK) - 4.18.0 64-bit

Oracle Linux 7.x (RHCK) - 3.10.0 build 957 64-bit

Oracle Linux 8.x (UEK) - 5.4.17 / 5.15.0 64-bit

Oracle Linux 8.x (RHCK) – 4.18.0 64-bit

Oracle Linux 9.x (UEK) – 5.15.0 64-bit

Oracle Linux 9.x (RHCK) – 5.14.0 64-bit



CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit

CentOS 8 Stream - 4.18.0 64-bit

CentOS 9 Stream - 5.14.0 64-bit

Fedora 37 – 40 – wsparcie do wygaśnięcia. 64-bit

AlmaLinux 8.x - 4.18.0 64-bit

AlmaLinux 9.x - 5.14.0 64-bit

Rocky Linux 8.x - 4.18.0 64-bit

Rocky Linux 9.x - 5.14.0 64-bit

CloudLinux 7.x - 3.10 (build 957) 64-bit

CloudLinux 8.x - 4.18.0 64-bit

Miracle Linux 8.x - 4.18.0 64-bit

Kylinv v10 RHEL - 4.19.90 64-bit

Oparte o Debian

Debian 9 - 4.9.0 32-bit/64-bit

Debian 10 - 4.19 32-bit/64-bit

Debian 11 - 5.10 32-bit/64-bit

Debian 12 – 6.1.0 64-bit

Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit

Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 64-bit

Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit

Ubuntu 22.04.x - 5.15 / 5.19 64-bit

Ubuntu 23.04.x – 6.2.0 64-bit

Ubuntu 24.04.x – 6.8.0 64-bit

PopOS 22.04.x – 6.2.6 64-bit

Pardus 21 – 5.10.0 64-bit

Mint 20.x – 5.4.0 64-bit

Mint 21.x – 5.15.0 64-bit

Mint 22.x – 6.8.0.x 64-bit

Zorin OS – 6.5.x 64-bit

Linux Mint Debian Edition 6 – 6.1.x 64-bit

Oparte o SUSE



SLES 12 SP4 - 4.12.14-x 64-bit
SLES 12 SP5 - 4.12.14-x 64-bit
SLES 15 SP1 - 4.12.14-x 64-bit
SLES 15 SP2 - 5.3.18-x 64-bit
SLES 15 SP3 - 5.3.18-x 64-bit
SLES 15 SP4 – 5.14.21 64-bit
SLES 15 SP5 – 5.14.21 64-bit
SLES 15 SP6 – 6.4.x 64-bit
SLED 15 SP4 – 5.14.21 64-bit
openSUSE Leap 15.4 - 15.5 - 5.14.21 64-bit

Cloud based Linux

AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x 64-bit
Amazon Linux v2 - 4.14.x / 4.19.x / 5.10 64-bit
Amazon Linux 2023 – 6.1.x 64-bit
Google COS Milestones 77, 81, 85 - 4.19.112 / 5.4.49 64-bit
Azure Mariner 2 - 5.15 64-bit

Linux dla ARM

Oparte o RPM

RHEL 8.x – 4.18.0-x
RHEL 9.x – 5.14
AlmaLinux 9.x – 5.14
Rocky Linux 9.x – 5.14

Oparte o Debian

Debian 11 – 5.10 / 6.1
Debian 12 – 6.1.0.x
Ubuntu 20.04.x – 5.15



Ubuntu 22.04.x – 5.15 / 5.19

Ubuntu 24.04.x – 6.8.0.x

Oparte o SUSE

SLES 15 SP4 – 5.14.21-x

openSUSE Leap 15.4-15.5 – 5.14.21-x

Oparte o chmurę

Amazon Linux v2 – 5.10

Amazon Linux 2023 - 6.1

Systemy Operacyjne Mac OS X

macOS Sequoia (15.x)

macOS Sonoma (14.x)

macOS Ventura (13.x)

macOS Monterey (12.x)

macOS Big Sur (11.x)

Obsługiwane Środowiska Microsoft Exchange

Security for Exchange wspiera następujące wersje i role Microsoft Exchange:

- Exchange Server 2019 z rolą Edge Transport lub Mailbox
- Exchange Server 2016 z rolą Edge Transport lub Mailbox
- Exchange Server 2013 z rolą Edge Transport lub Mailbox
- Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox

Network Attached Storage NAS

Przedmiotem zamówienia jest dostawa serwera NAS wraz z zainstalowanymi dyskami twardymi.

Specyfikacja sprzętowa	
Procesor	Procesor 64 bit x86 o takowaniu nie mniejszym niż 2.0 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 8GB
Pamięć Flash	Nie mniej niż 4 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
Wbudowane w urządzenie interfejsy na dyski M2	min. 2 x M2 PCIe Gen3x2
Możliwość stosowania dysków twardych o pojemności	do 20TB
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 2
Port HDMI	Tak, minimum 2
Przyciski	Reset, Zasilanie
Typ obudowy	Tower
Dopuszczalna temperatura pracy	od 0 do 40°C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilacz	Max. 90 W
Specyfikacja oprogramowania	
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak

Zarządzanie dyskami	<p>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</p>
Wbudowana obsługa iSCSI	<p>Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa MPIO Migawka / kopia zapasowa iSCSI LUN</p>
Zarządzanie prawami dostępu	<p>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</p>
Obsługa Windows AD	<p>Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP</p>
Funkcje backup	<p>Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,</p>
Współpraca z zewnętrznymi dostawcami usług chmury	<p>Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box</p>
Darmowe aplikacje na urządzenia mobilne	<p>Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android</p>
Minimum obsługiwane serwery	<p>Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediiów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu</p>
VPN	<p>VPN client / VPN server Obsługa PPTP, OpenVPN</p>



Administracja systemu	<p>Połączenia HTTP/HTTPS</p> <p>Powiadamianie przez e-mail (uwierzytelnianie SMTP)</p> <p>Powiadamianie przez SMS</p> <p>Ustawienia inteligentnego chłodzenia</p> <p>DDNS oraz zdalny dostęp w chmurze</p> <p>SNMP (v2 & v3)</p> <p>Obsługa UPS z zarządzaniem SNMP (USB)</p> <p>Obsługa sieciowej jednostki UPS</p> <p>Monitor zasobów</p> <p>Kosz sieciowy dla CIFS/SMB oraz AFP</p> <p>Monitor zasobów systemu w czasie rzeczywistym</p> <p>Rejestr zdarzeń</p> <p>System plików dziennika</p> <p>Całkowity rejestr systemowy (poziom pliku)</p> <p>Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line</p> <p>Aktualizacja oprogramowania automatyczna</p> <p>Możliwość aktualizacji oprogramowania ręcznie</p> <p>Ustawienia systemu: Kopia, Przywracanie, Resetowanie</p>
Wirtualizacja	<p>Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android.</p> <p>Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5</p> <p>Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.</p>
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia	<p>Filtracja IP</p> <p>Ochrona dostępu do sieci z automatycznym blokowaniem</p> <p>Połączenie HTTPS</p> <p>FTP z SSL/TLS (Explicit)</p> <p>Obsługa SFTP (tylko admin)</p> <p>Szyfrowanie AES 256-bit</p> <p>Szyfrowana zdalna replikacja (Rsync poprzez SSH)</p> <p>Import certyfikatu SSL</p> <p>Powiadomienia o zdarzeniach za pośrednictwem Email i SMS</p>
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Minimalny okres gwarancji	3 lata
Zainstalowane komponenty:	
Dyski HDD	<p>Dyski twarde przeznaczone do pracy ciągłej.</p> <p>Oferowane dyski muszą znajdować się na liście</p>



	<p>kompatybilności producenta z oferowanym urządzeniem i modulem rozszerzającym. Zamawiający wymaga dostarczenia 4szt. dysków o pojemności co najmniej 6 TB każdy. Prędkość obrotowa dysku minimum: 7000 obr/min Gwarancja na dyski minimum 50 miesięcy Średni czas bezawaryjnej pracy dysku minimum: 2 400 000 h</p>