I. Urządzenie do backupu/macierz do klastra HA – 3 szt. (cz. 1 zamówienia).

Typ urządzenia	Serwer NAS
Obudowa	Rack max. 1U
Procesor	Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark na sierpień 2022 co najmniej 4 580 punktów
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 16 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap z możliwością rozszerzenia do 8 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą portu eSATA.
Porty zewnętrzne	Minimum: • 2 porty USB 3.2.1 • 1 port eSATA (jako gniazdo rozszerzenia)
Porty sieciowe	Minimum: • 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego • 2 porty 10 GbE (dopuszcza się kartę rozszerzeń)
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 2.0	Min. 1x 4-liniowe gniazdo x8 gen. 3
Wentylator obudowy	Min. 3 wentylatory (40 × 40 × 20 mm)
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	• Maksymalny rozmiar pojedynczego wolumenu: 108 TB • Minimalny liczba wewnętrznych wolumenów: 64 • Minimalny liczba obiektów iSCSI Target: 128 • Minimalny liczba jednostek iSCSI LUN: 256 • Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	Minimalna liczba kont użytkowników: 2 048 • Minimalna liczba grup użytkowników: 256 • Minimalna liczba folderów współdzielonych: 512 • Minimalna liczba jednoczesnych połączeń CIFS/AFP/NFS/FTP: 2000
Uprawnienia	Uprawnienia listy kontroli dostępu systemu Windows® (ACL) i aplikacji
Wirtualizacja	Obsługa VMware vSphere with VAAI, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Integracja z usługami Windows® AD, logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP
Bezpieczeństwo	Zapora, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Obsługiwane przeglądarki	Google Chrome®, Firefox®, Microsoft Edge®, Safari® 13 i nowsze oraz Safari (iOS 13.0 i nowsze) na urządzeniach iPad, Chrome (Android™ 11.0 i nowsze) na tabletach
Oprogramowanie	Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów współdzielonych Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu

	(konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Konserwacja	Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack
Gwarancja	**• 3 lata na urządzenia główne**
Napędy	4 x 1,92TB SSD przeznaczone do pracy w urządzeniach typu NAS rekomendowanych przez producenta urządzenia NAS
Szyby do serwera	Dodatkowo wymagane są szyny do serwera NAS umożliwiające montaż w szafie RACK

II. Serwer – 2 szt. (cz. 2 zamówienia).

Obudowa

- Typu RACK, wysokość 2U;
- Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
- Opcjonalne ramię porządkujące kable z tyłu obudowy;
- Możliwość zainstalowania 16 dysków twardych hot plug 2,5";
- Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych;
- Zainstalowane 2 szt. dysków SSD M.2 480GB podłączone do sprzętowego kontrolera RAID;
- Możliwość zainstalowania dysku M.2 NVMe PCIe4.0 x4;
- Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.
- Możliwość zainstalowania dedykowanego wewnętrznego napędu LTO-8.

Płyta główna

- Dwuprocesorowa;
- Wyprodukowana i zaprojektowana przez producenta serwera;
- Możliwość instalacji procesorów 60-rdzeniowych;
- Zainstalowany moduł TPM 2.0;
- 6 złącz PCI Express generacji 5 w tym:
- 4 fizyczne złącza o prędkości x16;
- 2 fizyczne złącza o prędkości x8;
- Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
- Opcjonalnie możliwość uzyskania 9 aktywnych interfejsów PCI-e;
- 32 gniazda pamięci RAM;
- Obsługa minimum 8 TB pamięci RAM DDR5;
- Wsparcie dla technologii:
- Memory Scrubbing;
- SDDC;
- ECC;
- Memory Mirroring;
- ADDDC;
- Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.

Procesory

- Jeden procesor 16-rdzeniowy, taktowanie bazowe 2,8 GHz, architektura x86_64;
- osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 486 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org dla oferowanego serwera;

Pamięć RAM

- 64 GB pamięci RAM;
- DDR5 Registered 5600MT/s;

Kontrolery LAN

Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:

- 2x 1Gbit Base-T, w tym minimu 1 port dedykowany do zdalnego zarządzania serwerem OOB;
- 4x 10Gbit Base-T;
- Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;

Kontrolery I/O

- Kontroler SAS RAID dla dysków wewnętrznych, obsługujący poziomy RAID: 0,1,10,5;

Porty1

- Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
- 1 porty USB 3.0 wewnętrzny;
- 2 porty USB 3.0 dostępne z tyłu serwera;
- 2 porty USB 3.0 na panelu przednim;
- Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;

- Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

Zasilanie, chłodzenie

- Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W;
- Redundantne wentylatory hotplug.

Zarządzanie

- Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera – system przewidywania, rozpoznawania awarii;
- informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
- karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;
- procesory CPU;
- pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
- status karty zarządzającej serwera;
- wentylatory;
- bateria podtrzymująca ustawienia BIOS płyty głównej;
- zasilacze;
- system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);
- Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
- Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
- Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
- Dostęp poprzez przeglądarkę Web, SSH;
- Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
- Zarządzanie alarmami (zdarzenia poprzez SNMP);
- Możliwość przejęcia konsoli tekstowej;
- Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
- Obsługa serwerów proxy (autentykacja);
- Obsługa VLAN;
- Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
- Wsparcie dla protokołu SSDP;
- Obsługa protokołów TLS 1.2, SSL v3;
- Obsługa protokołu LDAP;
- Synchronizacja czasu poprzez protokół NTP;
- Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;
- Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii \ w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
- Wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
- Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

Wspierane OS

- Microsoft Windows Server 2025, 2022, 2019;
- VMWare vSphere 8.0;
- Suse Linux Enterprise Server 15;
- Red Hat Enterprise Linux 9, 8;
- Microsoft Hyper-V Server 2019.

Licencja na system operacyjny

Licencja na serwerowy system operacyjny w najnowszej udostępnionej produkcyjnie wersji, musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie 4 instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.

9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
   b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
   e. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
10. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
11. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
12. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
13. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
14. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
15. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
16. Mechanizmy logowania w oparciu o:
   a. Login i hasło,
   b. Karty z certyfikatami (smartcard),
   c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
17. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
20. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
21. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
22. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
23. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
   a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
   b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
      I. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
      II. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
      III. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
      IV. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
   c. Zdalna dystrybucja oprogramowania na stacje robocze.
   d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
   e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
      I. Dystrybucję certyfikatów poprzez http
      II. Konsolidację CA dla wielu lasów domeny,
      III. automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
      IV. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
      V. Szyfrowanie plików i folderów.
      VI. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
   f. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
   g. Serwis udostępniania stron WWW.
   h. Wsparcie dla protokołu IP w wersji 6 (IPv6),
   i. Wsparcie dla algorytmów Suite B (RFC 4869),
   j. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
   k. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
      I. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
      II. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
      III. Obsługi 4-KB sektorów dysków
      IV. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
      V. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
      VI. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
24. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
25. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
26. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
27. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

28. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
29. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Gwarancja

- Min. 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika serwisu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.
- Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
- Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
- Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).

Dokumentacja, inne

- Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;
- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;
- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;
- W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
- Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 8 - 85 %;
- Zgodność z normami: CB, RoHS, WEEE oraz CE.

Licencje dostępowe do oferowanych systemów operacyjnych umożliwiające dostęp do zasobów serwerów dla 20 urządzeń.

III. Przełącznik sieciowy – 2 szt. (cz. 3 zamówienia).

Nazwa elementu, parametru lub cechy		Opis wymagań
1.	Ilość portów 10/100/1000 Base-T RJ-45	Minimum 24
2.	Ilość portów SFP+	Minimum 4
3.	Opóźnienie 100 Mb, 1000 Mb, 10000 Mb	< 4.7 uSec, < 2.4 uSec, <1.3 uSec
4.	Opóźnienie 1000 Mb	< 2.4 uSec
5.	Rozmiar tabeli routingu (liczba wpisów statycznych)	Minimum 30
6.	Warstwa przełączania	Minimum L2+
7.	Wydajność przepustowa (Mpp)	Minimum 95 Mpps
8.	Zdolność przełączania	Minimum 125 Gb/s
9.	Wysokość przełącznika	1U
10.	Wielkość tablicy adresów MAC	Min. 15000 wpisów
11.	Częstotliwość procesora	Min. 800 Mhz
12.	Pamięć	Min. 512 MB SDRAM
13.	Pamięć flash	256GB
14.	Zgodność z normami	CISPR 24 / CISPR 35, EN 55024:2010 / EN 55035:2017, IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, IEC 61000-4-8, IEC 61000-4-11, EN 61000-3-2, IEC 61000-3-2, EN 61000-3-3, IEC 61000-3-3
15.	Protokół zdalnego zarządzania	SNMP 1, RMON, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, RADIUS
16.	Algorytm kodowania	SSL
17.	Metoda identyfikacji	RADIUS
18.	Cech	Sterowanie przepływem, obsługa DHCP, obsługa ARP, obsługa VLAN, auto-uplink (auto MDI/MDI-X), nasłuchiwanie IGMP, obsługa IPv6, tryb półdupleksu, tryb pełnego dupleksu, obsługa protokołu Spanning Tree (STP), obsługa protokołu Multiple Spanning Tree Protocol (MSTP), obsługa list dostępu (ACL), Quality of Service (QoS), Trusted Platform Module (TPM), obsługuje LLDP, Link Aggregation Control Protocol (LACP), Energy Efficient Ethernet, Class of Service (CoS), BPDU Filter, PoE Class 4
19.	Obsługa VLAN	Min. 250
20.	Trasy IP v4 (statyczne)	Min. 30
21.	Protokoły IEEE	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.2af, IEEE 802.3at, IEEE 802.3x, IEEE 802.1Q, IEEE

		802.1p, IEEE 802.3ad, IEEE 802.1X, IEEE 802.3az, IEEE 802.1D, IEEE 802.1W, IEEE 802.1S, IEEE 802.1AB
22.	Maksymalna moc znamionowa	37W
23.	Wbudowany zasilacz	Tak
24.	MTBF (lata)	Min. 150
25.	Dodatkowo	4 x wkładki SFP+
26.	Zużycie energii	Max. 23W W trybie bezczynności max. 10W
27.	Funkcja zarządzania	Przeglądarka internetowa, menedżer SNMP
28.	Gwarancja	**Min. 2 lata**

IV. UPS do serwerów – 2 szt. (cz. 4 zamówienia).

Nazwa elementu, parametru lub cechy	**Opis wymagań**
Moc pozorna	3000VA
Moc rzeczywista	3000W
Topologia (klasyfikacja IEC 62040-3)	Podwójna konwersja on-line z korekcją wejściowego współczynnika mocy systemu (PFC)
Sprawność przy pracy normalnej (100% obc.)	<92%
Współczynnik mocy	1
Czas przełączenia na baterię	0 ms
Liczba, typ gniazd wyjściowych	8 gniazd IEC C13 (10A) + 2 1 gniazdo IEC C19 (16A), w tym 2 zarządzane grupy wraz z pomiarem zużytej energii
Typ gniazda wejściowego	1 IEC C20 (16A) lub blok zacisków w wersji HotSwap MBP HW
Czas podtrzymania dla 100% obciążenia dla pf=1	3 min
Czas podtrzymania przy 50% obciążenia dla pf=1	10 min
Dodatkowe baterie	Możliwość dołożenia maksymalnie 4 zewnętrznych modułów bateryjnych
Napięcie znamionowe	220/230/240 V
Tolerancja napięci prostownika	176V-264V
Częstotliwość znamionowa	50/60 Hz autodetekcja
Tolerancja częstotliwości	40– 70 Hz
Kształt napięcia	Sinusoidalny
Napięcie znamionowe wyjściowe	230 V (domyślnie) / możliwość wyboru 220/240 V
Zakres zmian napięcia	+/-1% napięcia nominalnego
Częstotliwość wyjściowa	50/60 Hz +/-0,5%
Współczynnik szczytu	3:1
Dopuszczalny zakres współczynnika mocy obc. Liniowego	0,5 indukcyjny - 0,5 pojemnościowy
Baterie wymieniane przez użytkownika "na gorąco"	Tak
Ochrona przed przeładowaniem	Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
Ochrona przed głębokim rozładowaniem	Tak
Okresowy automatyczny test baterii	Tak
Zdolność zwarciowa	Min. 90A
Możliwość uruchomienia bez napięcia w sieci	Tak
Baterie wewnętrzne o pojemności nie mniejszej niż	9Ah 12V, minimum 6 szt.
Interfejs komunikacyjny	• USB
	• RS232 DB-9 żeński (HID)
	• 1 blok mini-zacisków do zdalnego wyłączania
	• 1 blok mini-zacisków przekaźnika wyjściowego
Panel sterowania z wyświetlaczem LCD	• Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe , częstotliwość wyjściowa), baterii (test baterii), pomiary i dane,napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii).
	• Poziomy rząd przycisków sterowania

	• Poziomy rząd wskaźników stanu : 4 LED
	• Sygnalizator akustyczny
Sygnały akustyczne	• Awaria
	• Niski stan naładowania baterii
	• Przeciążenie
	• Serwis
Przyciski sterujące i wskaźniki diodowe LED	• Escape (anulowanie)
	• Funkcyjne (przewijanie w górę i w dół)
	• Enter (potwierdzający)
	• ON/OFF załączenia i wyłączenia
	• LED trybu zasilania z siec i(kolor zielony)
	• LED trybu baterii (kolor żółty)
	• LED usterki (kolor czerwony)
	• LED w trybie obejścia (kolor pomarańczowy/niebieski)
Typ obudowy	Uniwersalna Tower/Rack 2U
Wyposażenie	UPS, instrukcja obsługi(CD), instrukcja bezpieczeństwa, instrukcja szybkiego montażu 1 x kabel szeregowy RS-232, 1 x kabel komunikacyjny USB 1 x kable wyjściowe IEC 16A 2 x kable wyjściowe IEC 10A uchwyty kablowe 1 x zestaw szyn montażowych 19' podstawki do montażu wieżowego
Dołączone oprogramowanie	Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie serwerów zasilanych z systemu i pracujących pod kontrolą systemów operacyjnych: - Windows: 7 / 8 / 2008 / Vista / 2003 / XP - Microsoft SCVMM 2012
Zgodność ze standardem Energy Star	Tak
Maksymalna szerokość	440 mm
Maksymalna wysokość	86,5 mm
Maksymalna głębokość	605 mm
Poziom hałasu w odl. 1m	<55 dla pracy normalnej
Znaki bezpieczeństwa	CE, IEC/EN 62040-1, IEC/EN 62040-2:
Gwarancja producenta	**3 lata na elektronikę**, 2 lata na baterie akumulatorów
Karta sieciowa	Zainstalowana karta sieciowa

V. Urządzenie typu UTM (cz. 5 zamówienia).

Parametr	Minimalne wymagania
Porty	1 x WAN 10/100/1000 + 4 x LAN 10/100/1000
Przepustowość IPS	1 Gb/s
Przepustowość NGFW	800 Mb/s
Przepusutść Threat Protection	600 Mb/s
Przepustowość Firewalla	5 Gb/s
Opóźnienie zapory (64 bajtowe pakiety)	4 µs
Przepustowośc zapory (liczba pakietów na sekundę)	7.5 Mpps

Sesje równoległe (TCP)	700 000
Nowe sesje na sekundę (TCP)	35 000
Firewall Policies	5 000
Przepustowość IPsec VPN (512 bajtów)	4.4 Gb/s
Tunele IPsec typu Brama-Brama	200
Tunele IPsec typu Klient-Brama	250
Przepustowość SSL-VPN	490 Mb/s
Liczba użytkowników SSL-VPN (zalecana)	200
SSL Inspection Throughput (IPS, avg. HTTPS)	310 Mb/s
SSL Inspection CPS (IPS, avg. HTTPS)	320
Ilość Sesji SSL Inspectio (IPS, avg. HTTPS)	55 000
Przepustowość kontroli aplikacji (HTTP 64K)	990 Mb/s
Przepustowość CAPWAP (HTTP 64 KB)	3.5 Gb/s
Domeny wirtualne (domyślne / maksymalne)	10/10
Licencja na reguły i aktualizację	roczna licencja 24x7 na aktualizacje firmware oraz reguły IPS/antywirus/web filtring/antispam
Wsparcie	roczne wsparcie producenta nie później niż na następny dzień roboczy z urządzeniem zastępczym
Funkcjonalności	1. VPN – zarówno IPSec dedykowany dla szyfrowanych połączeń pomiędzy lokalizacjami jak i SSL-VPN jako bezpieczne połączenie dla użytkowników mobilnych 2. Kontrola aplikacji rozpoznająca je na podstawie głębokiej analizy z możliwością przydzielania priorytetów obsługi dla poszczególnych użytkowników, przypisania ich do konkretnego łącza, itd. 3. Skanowanie antywirusowe z wykorzystaniem bazy sygnatur oraz heurystyki, także dla ruchu szyfrowanego poprzez inspekcję SSL 4. Filtr stron www kontrolujący jaki użytkownik, kiedy i z jakim priorytetem może korzystać z danej kategorii stron lub konkretnej domeny 5. System zapobiegania włamaniom IPS 6. Antyspam zabezpieczający przed niechcianą pocztą poprzez protokoły IMAP(S), POP3(S) oraz SMTP(S) 7. System chroniący przed wyciekiem danych DLP monitorujący ruch pod kątem przesyłania danych wrażliwych 8. Wysoka dostępność realizowana poprzez konfigurację klastrów urządzeń w trybie active-active lub active-passive 9. Skaner podatności sieci umożliwiający sprawdzenie serwerów i stacji końcowych pod kątem luk bezpieczeństwa 10. Identyfikacja urządzeń końcowych umożliwiająca ich kontrolę poprzez przydzielanie odpowiednich polityk dostępowych (BYOD) 11. Kontroler sieci bezprzewodowej klasy enterprise pozwalający na zarządzanie punktami dostępowymi jednocześnie zapewniając bezpieczeństwo dostępu niespotykane w konkurencyjnych rozwiązaniach 12. Dwuskładnikowe uwierzytelnianie 13. Możliwość rozbudowy urządzenia o zewnętrzny modem 4G/LTE firm trzecich 14. możliwość zarządzania wieloma łączami w celu zapewnienia wysokiej dostępności WAN 15. Integracja z systemami wykrywania i przeciwdziałania nieznanym zagrożeniom dzięki technologii sandbox
Gwarancja	**Min. 1 rok**

VI. Oprogramowanie do zarządzania komputerami – na 20 stanowisk (cz. 6 zamówienia).

Oprogramowanie musi składać się z co najmniej pięciu modułów:

1. Modułu do monitorowania infrastruktury (bezagentowo) powinien obsługiwać serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

- wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
- wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)
- wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku.
- wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze.
- wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie.
- wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny.
- zablokowania mapy urządzeń przed przypadkową edycją.
- serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów.
- serwerów pocztowych:
  - program powinien monitorować czas logowania do serwisu odbierającego oraz czas wysyłania poczty,
  - program powinien mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),
  - program powinien mieć możliwość wykonywania operacji testowych, - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa.
- monitorowania serwerów WWW i adresów URL.
- cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS.
- obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.
- obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID.
- obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych.
- monitoringu routerów i przełączników wg:
  - zmian stanu interfejsów sieciowych,
  - ruchu sieciowego,
  - podłączonych stacji roboczych
  - graficzna prezentacja panelu switcha,
  - ruchu generowanego przez podłączone do portów stacje robocze.
- serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie.
- wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu.
- wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

2. Moduł do inwentaryzacji - program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:
   - prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
   - obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
   - Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows.
   - zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
   - posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
   - umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
   - umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
   - umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
   - umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
   - umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.

   Moduł inwentaryzacji zasobów powinien umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i oprogramowania:

   - przechowywanie wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatyczne aktualizowanie zgromadzonych informacji,
   - tworzenie powiązań między zasobami a urządzeniami,
   - tworzenie powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
   - wskazanie osób uprawnionych do użycia zasobów,
   - definiowanie własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania powinna być możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu, nazwa firmy serwisującej, lub własny komentarz,

- określenie atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
- określenie atrybutów dodatkowych tylko dla wybranych typów zasobów,
- definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
- importu danych z zewnętrznego źródła (.CSV),
- przechowywanie dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
- tworzenie powiązań między zasobami a dokumentami w relacji 1:N,
- oznaczanie statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
- ewidencje czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
- generowanie zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
- generowanie protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
- archiwizacje i porównywania audytów zasobów,
- worzenie kodów kreskowych dla zasobów,
- drukowanie kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
- inwentaryzacje zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej na system Android,
- inwentaryzacje stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
- definiowanie alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data" z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja").

Inwentaryzacja oprogramowania powinna zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

- skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. 2
- informacje o aplikacjach używanych w organizacji.
- tworzenie własnych wzorców aplikacji.
- tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
- informacje o komputerach, na których aplikacja została wykryta.
- zarządzanie posiadanymi licencjami.
- wskazywanie osób odpowiedzialnych za licencję.
- wskazanie użytkowników licencji.
- tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
- rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
- łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
- zarządzanie posiadanymi licencjami: raport zgodności licencji.
- możliwość przypisania do programów numerów seryjnych, wartości itp.

Okna audytowe powinny posiadać możliwość filtrowania elementów per oddział.

3. Moduł OBSŁUGI UŻYTKOWNIKÓW powinien umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:
   - Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
   - Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
   - Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
   - Informacji o edytowanych przez użytkownika dokumentach,
   - Historii pracy (cykliczne zrzuty ekranowe),
   - Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),
   - Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
   - Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
   - Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

   Moduł ponadto powinien posiadać możliwość:

   - wykrywania podejrzanej aktywności przez popularne „jigglery", mającej na celu symulowanie faktycznej pracy.
   - definiowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.
   - wyszczególnienia podejrzanej aktywności w raportach.
   - wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności.
   - automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności.
   - blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami.
   - integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT.
   - skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia.

- automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych.
- blokowania ruchu na wskazanych portach TCP/IP,
- blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
- prowadzenia rejestru naruszeń blokad,
- wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,
- przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
- definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone

4. Moduł pomocy zdalnej powinien umożliwiać:
   Kontrolę stacji użytkownika poprzez podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator powinni widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu powinien mieć możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu powinna umożliwiać równoczesne podłączenie do tego samego komputera kilku administratorom. Dodatkowo powinien umożliwiać:
   - pobieranie listy użytkowników z Active Directory wraz z awatarami,
   - wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym,
   - zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
   - zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
   - zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń,
   - zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy,
   - tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,
   - automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,
   - definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,
   - przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,
   - procesowanie zgłoszeń użytkowników z wiadomości e-mail,
   - dostęp do plików źródłowych wiadomości e-mail przetworzonych na zgłoszenia,
   - obsługę wielu adresów e-mail jednego użytkownika w celu przetwarzania jako zgłoszeń pochodzących od tej samej osoby,
   - eksportowania listy zgłoszeń do plików CSV i XLSX,
   - integrację ze wieloma skrzynkami e-mail w celu obsługi różnych kanałów zgłoszeń wraz z automatyzacjami,
   - integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,
   - tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
   - wykonywanie operacji na wielu zgłoszeniach równocześnie,
   - dołączanie załączników do zgłoszeń,
   - usuwanie zamkniętych zgłoszeń,
   - rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
   - szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
   - wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
   - zrzuty ekranowe (podgląd pulpitu),
   - zdalną modyfikację rejestrów,
   - dystrybucję oprogramowania przez Agenty,
   - definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,
   - przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,
   - dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
   - zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
   - możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
   - możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy,
   - planowanie nieobecności pracowników helpdesk,
   - obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,
   - generowanie raportów obsługi helpdesk,
   - zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),
   - zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
   - wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.
5. Moduł OCHRONY DANYCH PRZED WYCIEKIEM powinien umożliwiać:

- Blokowanie urządzeń i nośników danych. Moduł powinien umożliwiać zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
- Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
- Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
- Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
- Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
- Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
- Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
- Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
- Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.
- Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
- Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.
- Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Zarządzanie prawami dostępu do urządzeń:

- Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
- Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.
- Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
- Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
- Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:

- Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
- Podłączenie/odłączenie urządzenia przenośnego.

VII. Zakup rozszerzenia licencji o numerze EAV-84299578 do wersji ESET Protect Elite, licencja na okres 1 roku (cz. 7 zamówienia).

Zakup rozszerzenia dotyczy licencji już posiadanej przez Zamawiającego, dlatego też została wskazana nazwa konkretnego oprogramowania.