Zał. Nr 5 do SWZ - Opis przedmiotu zamówienia

Część I – wyposażenie serwerowni i oprogramowanie

1. W ramach dostawy wyposażenia mają zostać dostarczone:
    1) serwer do tworzenia kopii zapasowych wraz z osprzętem i systemem operacyjnym – 1 szt.,
    2) serwer plików NAS z macierzą do przechowywania plików użytkowników – 1 szt,
    3) serwer plików NAS z macierzą do przechowywania plików Urzędu – 1 szt,
    4) serwer do zarządzania infrastrukturą z systemem operacyjnym i osprzętem – 1 szt.,
    5) przełączniki sieciowe – 10 szt.,
    6) zasilacze UPS – 18szt
    7) oprogramowanie antywirusowe - upgrade obecnego oprogramowania,
    8) oprogramowanie do zarządzania infrastrukturą IT.
2. Wymagania ogólne dla urządzeń i oprogramowania:
    1) Całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów na rynek polski;
    2) Całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana we wcześniejszych projektach;
    3) Całość sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producenta sprzętu, niezależnie od statusu partnerskiego Wykonawcy przez okres 24 miesięcy (chyba, że zapisy szczegółowe stanowią inaczej);
    4) Zamawiane licencje powinny pochodzić z legalnego źródła, powinny być nowe i nieużywane wcześniej. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.
3. Warunki gwarancji i wsparcia technicznego dla sprzętu i oprogramowania sieciowego:
    1) ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona min. 2-letnia gwarancja (chyba, że zapisy szczegółowe stanowią inaczej) oparta na gwarancji producenta; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
    2) Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon, fax, e-mail lub WWW (przez całą dobę);
    3) W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający dopuszcza podstawienie na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
    4) Zamawiający wymaga świadczenia opieki serwisowej przez okres min. 12 miesięcy z czasem reakcji na zaistniałe problemy wynoszącym 4 godziny. Czas reakcji jest rozumiany jako podjęcie działań mających na celu rozwiązanie zaistniałych problemów technicznych.
    5) Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Wykonawcy;

UWAGA. Powyższe zapisy gwarancyjne, oraz czas wykonania obowiązują jedynie w przypadku braku szczegółowych zapisów w poniższym opisie przedmiotu zamówienia.

4. Miejsce Instalacji
    1) Dostawa, montaż i instalacja w ramach niniejszego postępowania przetargowego odbędzie się w czasie i miejscu wskazanym przez Zamawiającego.
5. Montaż i uruchomienie
    1) Zamawiający wymaga aby wraz z dostawą sprzętu przeprowadzić jego instalację, konfigurację oraz uruchomienie. Wszelkiego typu niezbędne elementy np.: patchcordy światłowodowe, korytka, wkładki SFP+ itp. powinny zostać ujęte w wycenie.
    2) Przekazanie elementów systemu nastąpi w drodze protokołu przekazania do użytkowania, który będzie potwierdzał jego prawidłową instalację i działanie.
    3) Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji.
    4) Zamawiający wymaga usunięcia opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
    5) Podłączenie całości rozwiązania do infrastruktury Zamawiającego.
    6) Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
    7) Wykonanie procedury aktualizacji firmware urządzeń Zamawiającego do najnowszej wersji oferowanej przez producenta sprzętu.
    8) Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie.
    9) Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające). Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia, w ramach jednego weekendu (Piątek godz. 16:00 – Sobota godz. 22:00) po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Zamawiającym.
    10) Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci dwóch osób w siedzibie Zamawiającego w ciągu 7 dni następujących po pracach wdrożeniowo – instalacyjnych w godzinach od 7.30 do 15.30. W tym czasie przedstawiciele Wykonawcy zobowiązani są do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji. W tym czasie przedstawiciele Wykonawcy dokonają także przeszkolenia dwóch pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań.
    11) Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Zamawiający jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu.

6. Wymagania szczegółowe

1. Oprogramowanie antywirusowe – wymagania minimalne

Wymagania ogólne	**W ofercie należy podać nazwę producenta, nazwę produktu oraz wersję** umożliwiające jednoznaczną identyfikację oferowanego oprogramowania.
Ilość licencji	35
Wymagany okres trwania licencji	24 miesiące
Wymagane wspieranie	Windows 11 October 2023 Update (23h2); Windows 10 November 2022 Update (22H2); Windows 11 September 2022 Update (22H2); Windows 11

systemów operacyjnych - komputerowych	(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
Wymagane wspieranie systemów operacyjnych – tablety i 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
Wymagane wspieranie systemów operacyjnych - serwerowych	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
Wymagane wspieranie systemów operacyjnych Linux	RHEL 7.x - 3.10.0 (build 957) 64-bit; RHEL 8.x - 4.18.0 64-bit RHEL 9x - 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 36 – 38 – 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; Kylinv10 RHEL - 4.19.90 64-bit; 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 6 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; 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 – 5.15.0 64-bit 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; openSUSE Leap 15.2 - 15.4 - 5.3.18 / 5.14.x 64-bit;

	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 RHEL 8.x – 4.18.0-x; RHEL 9.x – 5.14; AlmaLinux 9.x – 5.14; Rocky Linux 9.x – 5.14 Debian 11 – 5.10 / 6.1; Ubuntu 20.04.x – 5.15; Ubuntu 22.04.x – 5.15 / 5.19 SLES 15 SP4 – 5.14.21-x; openSUSE Leap 15.4 – 5.14.21-x Amazon Linux v2 – 5.10; Amazon Linux 2023 - 6.1
Wymagane wspieranie systemów operacyjnych MAC OS	macOS Sonoma (14.x); macOS Ventura (13.x); macOS Monterey (12.x); macOS Big Sur (11.x)
Obsługiwane Środowiska 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 Oferowane oprogramowanie musi być kompatybilne z Microsoft Exchange Database Availability Groups (DAG).
Ochrona środowisk wirtualnych (SVE)	- Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej - Maszyna wirtualna pełniąca rolę silnika skanującego może być pobrana w formacie: OVA; XVA; VHD; VMDK
Wspierane środowiska wirtualne	VMware vSphere and vCenter Server wersje: 6.5, 6.7, zawierająca aktualizację 1, 2a i 3; 7.0, zawierająca aktualizację 1, 2, 2b, 2c i 2d; 8.0, zawierająca aktualizacje 1, 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 (zawierająca Hyper-V Hypervisor) Red Hat Enterprise Virtualization 3.0 (zawierająca 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 z AHV 20170830.115, 20170830.301, 20170830.395 i 20190916.294 (Community Edition)

Wymagany poziom ochrony antywirusowej i antyspyware	- Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami - Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim. - Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi - Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog. - Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. - Wbudowana technologia do ochrony przed rootkitami. - Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. - Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". - Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. - Program powinien mieć możliwość dodawania wykluczeń na podstawie: pliku, folderu, rozszerzenia, procesu, hash pliku, hash certyfikatu, nazwy zagrożenia, wiersza poleceń, IP/maski - Powinno być zapewnione skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express. - Powinna być możliwość skanowania i oczyszczania poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). - Zamawiający wymaga automatycznej integracji skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. - Powinna być możliwość skanowania ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch powinien być automatycznie blokowany, a użytkownikowi wyświetlane powinno być stosowne powiadomienie. - Program powinien zapewnić blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych powinien móc określać administrator. Dodatkowo zdefiniowane przez producenta powinny być grupy stron. - Powinna być zapewniona automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. - Program powinien dawać możliwość definiowania, czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać. - Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH - Program powinien skanować ruch HTTPS transparentnie, bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. - Program powinien mieć możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program będzie pytał o hasło. - Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji: O programie” powinna być możliwość zdefiniowania przez administratora

	danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony. - W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników. - W GUI programu możliwość wyświetlenia, kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia. - Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. - Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. - Praca programu musi być niezauważalna dla użytkownika. - Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej. - Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet. - Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej. - Możliwość odblokowania ustawień programu po wpisaniu hasła. - Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu. - Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie). - Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu. - Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp. - Funkcja Ochrony danych konfigurowana zdalnie przez administratora. - Jedna wersja instalacyjna na stacje robocze i serwery plików Windows. - Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego. - Wbudowany IDS - Możliwość zainstalowania silnika pełnego, lekkiego ze sprawdzaniem reputacji plików w chmurze lub wykorzystanie dodatkowej maszyny wirtualnej która przejmie rolę silnika skanującego. - Maszyna, która przejmuję rolę silnika skanującego musi działać w trybach redundancji lub równej dystrybucji. - W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników. - W GUI programu możliwość wyświetlenia, kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia. - Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. - Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.

	- Praca programu musi być niezauważalna dla użytkownika. - Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej. - Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet. - Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej. - Możliwość odblokowania ustawień programu po wpisaniu hasła. - Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu. - Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie). - Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu. - Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp. - Funkcja Ochrony danych konfigurowana zdalnie przez administratora. - Jedna wersja instalacyjna na stacje robocze i serwery plików Windows. - Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego. - Wbudowany IDS - Możliwość zainstalowania silnika pełnego, lekkiego ze sprawdzaniem reputacji plików w chmurze lub wykorzystanie dodatkowej maszyny wirtualnej która przejmie rolę silnika skanującego. - Maszyna, która przejmuję rolę silnika skanującego musi działać w trybach redundancji lub równej dystrybucji. - Aktualizacja maszyny skanującej musi obejmować oddzielną aktualizację nowych funkcji, ulepszeń, poprawek oraz oddzielną aktualizację systemu operacyjnego urządzenia wirtualnego. - Możliwość tworzenia list sieci zaufanych. - Możliwość dezaktywacji funkcji zapory sieciowej. - Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu. - Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware. - Mechanizm, który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji.

	- Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa) - Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups - Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego. - System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system, który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać: - Funkcję, która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji: ochrony przeglądarki internetowej; sieć i poświadczenia; błędna konfiguracja systemu operacyjnego; - System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe: System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk, system, który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie; system pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania; system pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach; system pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie - 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: wymuszenie funkcji DEP systemu Windows, wymuszenie relokacji modułów (ASLR) (ta warstwa zabezpieczeń dotyczy systemów opartych na systemie Windows) - Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochroną przed technikami takimi jak: wczesny dostęp, dostęp do poświadczeń, wykrycie, crimeware - 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. - Formaty plików jakie mogą być odzyskane: 3fr|ai|arw|bay|cab|cdr|cer|cr2|crt|crw|dcr|der|dgn|dll|dng|doc|docm|docx|dwg|dxf|dxg|eps|erf|exe|indd|ini|jpe|jpeg|jpg|mdf|mef|mrw|msg|msi|nef|nrw|odb|odc|odm|odp|ods|odt|orf|p12|p7b|p7c|pdd|pdf|pef|pem|pfx|png|ppt|pptm|pptx|psd|pst|ptx|py|r3d|raf|rtf|rw2|rwl|sr2|srf|srw|tsf|wb2|wpd|wps|x3f|xlk|xls|xlsb|xlsm|xlsx|xml|

	- Oprogramowanie ma dawać możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania. - Ochrona proaktywna ma być oparta o maszynowe uczenie, które działa w fazie poprzedzającej wykonanie, ochrona ta musi wykrywać zagrożenia takie jak: ukierunkowane ataki, podejrzane pliki i ruch w sieci, exploity, ransomware, grayware - Moduł ochrony proaktywnej musi posiadać oddzielne działania, jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego - Moduł ochrony proaktywnej musi działać w trybach, które administrator może dowolnie zmieniać na: tolerancyjny, normalny, agresywny - Zintegrowany sandbox po stronie producenta, który pozwala na analizę pliku. Plik powinien móc zostać wysłany automatycznie ze stacji roboczej, jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora; powinna być możliwość przesłania archiwum zabezpieczonego hasłem; możliwość przesłania adresu URL; w przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo. - Wbudowany sandbox musi działać w trybie monitorowania i blokowania, musi oferować działania naprawcze takie, jak dezynfekcja lub przeniesienie do kwarantanny, musi oferować opcję wstępnego filtrowania zawartości, która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania, musi posiadać opcję, która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa. - Minimalny rozmiar pliku jaki może zostać przesłany do sandboxa to 1KB, maksymalny rozmiar pliku jaki może zostać przesłany do sandboxa to 50MB. - Powinna być możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM Splunk (wymaga TLS 1.2 lub wyższy). - Oprogramowanie ma pozwalać na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników zagrożeń. - Oprogramowanie musi skanować nośniki USB, zanim użytkownik zaloguje się do systemu Windows. - System musi wykrywać podatne sterowniki zainstalowane na punkcie końcowym - Agent i usługi oprogramowania antywirusowego zainstalowanego na punkcie końcowym muszą być chronione przed próbami manipulacji i naruszenia ich integralności. - System musi umożliwiać skanowanie oprogramowania układowego UEFI
Wymagania dotyczące maszyn wirtualnych	- Powinna być możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienia informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu); możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej; możliwość zabezpieczenia hasłem klienta przed odinstalowaniem; wersja kliencka nie musi pełni roli ochrony antywirusowej, a tylko być agentem dla Security Servera; dla maszyn z systemem Linux powinna być możliwość wskazania katalogów, które mogą być chronione w czasie rzeczywistym; możliwość określenia co jaki czas mają być wysyłane pliki z kwarantanny do producenta; po aktualizacji sygnatur baz antywirusowych powinna być dostępna opcja automatycznego przeskanowania

	kwarantanny; możliwość wskazania do jakiego serwera ochrony mają się łączyć klienci maszyn wirtualnych.
Wymagania dotyczące stacji roboczych i serwerów Windows	- Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. - Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. - Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. - Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". - Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. - Skanowanie plików spakowanych i skompresowanych. - Oprogramowanie powinno zawierać monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego. - Oprogramowanie powinno posiadać możliwość zablokowania hasłem odinstalowania programu. - Produkt oraz sygnatury muszą być aktualizowane nie rzadziej niż raz na godzinę. - Oprogramowanie musi posiadać możliwość raportowania zdarzeń informacyjnych. - Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju. - Program musi posiadać możliwość skanowania jedynie nowych niezmienionych plików. - Program musi mieć wbudowany skaner wyszukiwania rootkitów - Możliwość odblokowania ustawień programu po wpisaniu hasła - Możliwość uruchomienia zadania skanowania z niskim priorytetem - Możliwość wykorzystania dodatkowej maszyny wirtualnej która przejmie role silnika skanującego. - Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej. - Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem - Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym. - Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
Ochrona Exchange	- Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego. - 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 przeciągu ostatnich kilku godzin / dni.

	- Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz nie możliwych do przeskanowania. - Możliwość wykluczenia potencjalnie niechcianych aplikacji (PUA) z filtrowania antymalware. - Możliwość skanowania w poszukiwania malware wewnątrz archiwów. - Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen. - Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera. - Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy. - Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi. - Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowania maila do konkretnej skrzynki pocztowej. - 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. - 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	- Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows. - Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego. - Możliwość integracji wielu domen Active Directory - Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych. - Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki). - Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi - Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego. - Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu. - Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej. - Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.

	- Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej. - Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv. - Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip. - Możliwość generowania raportu co godzinę. - Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu. - Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej. - Możliwość dodania etykiety do stacji roboczej. - Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej. - Możliwość przechowywania kwarantanny maksymalnie 180 dni - Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać. - Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny. - W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej. - Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym.[2] - Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania. - 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. - Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia 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 - Integracja z serwerem Syslog. - Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238 - Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni. - Możliwość zablokowania konta w konsoli, xjeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem. - Funkcja pojedynczego logowania – Single Sign-on (SSO). - Możliwość naprawy instalacji z poziomu konsoli. - Raport streszczający - Możliwość podglądu raportu, który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak: zarządzane punkty

	końcowe, aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne, pięć najczęściej blokowanych zagrożeń, podział zagrożeń na urządzenia takie jak stacje robocze i serwery, status incydentów bezpieczeństwa, które wystąpiły, stan modułów punktów końcowych, ocena ryzyka firmy, zablokowane strony WWW w oparciu o wykryte tam szkodliwe programowanie, phishing, oszustwa, zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware - Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak: pakiety, sieć, kwarantanna, licencjonowanie, integracje, polityki, raporty, konta, firmy - 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 pozwala na określenie godziny, kiedy te maszyny będą usuwane - Możliwość określenia własnego serwera NTP. - Integracja z vCenter Server, z Xen Server, z nutanix Prism Element, Amazon EC2, z Azure. - Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony. - Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego. - Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej. - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej, dostępne muszą być opcje takie jak: lotnictwo, rolnictwo, automotive, usługi komercyjne, doradztwo, energia, usługi finansowe, rząd, opieka zdrowotna, technologie, transport, non-profit, górnictwo, media - Funkcja kontroli aplikacji, która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów i może działać w trybie testowym lub produkcyjnym,

	pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat. - Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta. - Możliwość wyświetlenia czy punkt końcowy jest serwerem, czy stacją roboczą. - Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS. - Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym. - Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni. - Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS. - Oprogramowanie ma umożliwiać pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1. - Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych. - Oprogramowanie ma umożliwiać ochronę kontenerów instalowaną bezpośrednio na hoście kontenera, oferować wgląd w złośliwą aktywność serwera Linux i kontenerów w czasie rzeczywistym. - Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Program wczesnego dostępu powinien umożliwiać testowanie najnowszych funkcji oprogramowania których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe. - Oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Oprogramowanie musi umożliwiać przypisywanie znaczników ręcznie lub automatycznie. Oprogramowanie musi umożliwiać filtrowanie punktów końcowych na podstawie wybranych znaczników, musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie. - System umożliwia pobieranie plików poddanych kwarantannie z poziomu centralnej konsoli administracyjnej.
Wymagania do funkcjonalności EDR-Endpoint Detection and Response	- Produkt ma zapewniać szczegółowe informacje o wykrytych incydentach, interaktywną mapę incydentów i działania naprawcze. - Ma wspierać systemy operacyjne: A. Systemy desktopowe • 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 B. Systemy operacyjne dla serwerów: • 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 C. MacOS: • macOS Sonoma (14.x) • macOS Ventura (13.x) • macOS Monterey (12.x) • macOS Big Sur (11.x) D. Linux • RHEL 7.x - 3.10.0 (build 957) 64-bit • RHEL 8.x - 4.18.0 64-bit • RHEL 9x - 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 36 – 38 – 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

	• Kylinv10 RHEL - 4.19.90 64-bit • 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 6 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 • 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 – 5.15.0 64-bit • 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 • openSUSE Leap 15.2 - 15.4 - 5.3.18 / 5.14.x 64-bit • 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 - Wymagane główne elementy funkcjonalności EDR: Czujnik EDR, który gromadzi i przetwarza dane w celu raportowania danych dotyczących punktu końcowego i zachowania aplikacji; Security Analytics, komponent służący do interpretacji metadanych gromadzonych przez czujnik EDR; Możliwość instalacji dodatkowego, lekkiego agenta z czujnikiem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną ochronę. Agent powinien posiadać też ochronę urządzenia i ruchu sieciowego oraz filtr stron internetowych.
EDR – wymagania dotyczące wykrywania podejrzanej aktywności	- Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności. - Bazowanie na systemach bazujących na wskaźnikach ataku MITRE i własnej inteligencji. - Zgłaszanie wszystkich naruszeń jako incydent w module EDR.
EDR- wymagania dotyczące incydentów i wizualizacji	- Produkt ma zapewniać wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym przedziale czasu. - Produkt ma integrować się z bazą wiedzy ATT & CK firmy MITRE i odpowiednio oznaczać zdarzenia bezpieczeństwa. - Produkt ma zapewniać zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi informacjami lub działaniami z następującymi informacjami: karta Podsumowanie ma zawierać przegląd wpływu zdarzenia i szczegółowe

	informacje o każdym węźle zdarzenia, funkcja osi czasu ma zbierać informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej, działania naprawcze mają gromadzić informacje o działaniach blokujących automatycznie podejmowanych przez produkt w związku z bieżącym zdarzeniem bezpieczeństwa.
EDR – wymagania dotyczące działań związanych z incydentami	- Oprogramowanie ma pozwalać na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i linii zdarzeń oraz dawać możliwość: filtrowania zdarzeń, blokowania procesów, dodawania procesów do czarnej listy, dodawania procesów do białej listy, izolacji hosta, aktualizacji oprogramowania firm trzecich na hoście (wymagany add-on), przesłania pliku do Sandbox, sprawdzenia informacji o pliku w Google, sprawdzenia informacji o pliku w VirusTotal - Filtrowanie zdarzeń musi odbywać się na oceny zagrożenia od 10 do 100 punktów, daty wykrycia, statusu, ID, nazwy punktu końcowego, typu ataku (ransomware, potencjalnie niechciana aplikacja, malware, exploit, fileless, password stealer, downloader, inne, zdefiniowane przez użytkownika) - Możliwość szybkiego podglądu otwartych incydentów, najczęstszych powiadomień, urządzeń, które mają najczęściej problem. - Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie. - Możliwość wyświetlenia zablokowanych hashy plików. - Możliwość dodania własnych hashy MD5 oraz SHA256 - Możliwość importu hashy z pliku CSV - Możliwość filtrowania dodanych hashy na podstawie: Typu hashu, wartości hash, źródło dodania, informacje o źródle, nazwa pliku, firma, której dotyczy wpis, możliwość wyświetlenia 10,20,30,50,100 wpisów na jednej stronie.
Dodatkowe wymagania odnośnie funkcjonalności konsoli	- wymagana jest konsola On-premise – lokalny serwer administracyjny - Integracja z serwerem Syslog. - Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog. - Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym. - Możliwość określenia własnego serwera NTP. - Integracja z vCenter Server, z Xen Server, z nutanix Prism Element, z Azure. - Funkcja kontroli aplikacji, która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów. Funkcja kontroli aplikacji może działać w trybie testowym lub produkcyjnym. Funkcja kontroli aplikacji pozwala na

	zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat. - Filtrowanie zdarzeń odbywa się na podstawie: ocena zagrożenia od 10 do 100 punktów, data wykrycia, status, ID, nazwa punktu końcowego, typ ataku (ransomware, potencjalnie niechciana aplikacja, malware, exploit, fileless, password stealer, downloader, inne, zdefiniowane przez użytkownika) - Wyszukiwanie zdarzeń ma odbywać się na podstawie: Nazwa alertu, IP punktu końcowego, Hash MD5, Hash SHA256, nazwa użytkownika

2. Serwer NAS – z macierzą do przechowywania plików użytkowników - **1 szt.**

Wymagania ogólne	**W ofercie należy podać nazwę producenta i model** umożliwiające jednoznaczną identyfikację oferowanego produktu.
Procesor	Czterordzeniowy procesor typu ARM o częstotliwości min. 1,7GHz, 64-bitowy, uzyskujący w benchmarku wynik na poziomie przynajmniej 1150 pkt. (https://www.cpubenchmark.net/)"
Obudowa	Rack 2U o wymiarach, 89(H) x 482(W) x 534(D) mm, wraz z kompletem szyn teleskopowych
Ilość slotów RAM	Minimum 1x Long-DIMM DDR4
Pamięć RAM	Minimum 4GB UDIMM DDR4, z możliwością rozbudowy do 16GB
Pamięć Flash	Min. 512 MB
Ilość obsługiwanych dysków	Min. 8 dysków 2.5"/3.5" SATA3 Hot Swap
Ilość dysków zamontowanych	8 dysków 3,5-cala HDD, min. 6TB SATA, 5400RPM, 256MB cache, min. 1 mln h MTBF, przeznaczony do pracy 24/7, gwarancja producenta min. 3 lata
Interfejsy sieciowe	Minimum 2 x Port 2,5 Gigabit (2,5G/1G/100M), 2 x 10 GbE SFP+
Porty	Min. 4x USB 3.2 Gen 1, 1 x PCIe Gen 2 x2
Wskaźniki LED	HDD 1-8, stan, LAN, Power, USB
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0,1,5,5+Spare,6,6+Spare,10,10+Spare,50/60.
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online. Przywracanie RAID.
Szyfrowanie	Możliwość szyfrowania folderów współdzielonych oraz całych woluminów kluczem AES 256 bitów. Mechanizm szyfrowania z akceleracją sprzętową.
Wspierane systemy operacyjne	Windows 7, Windows 8, Windows 10, Windows Server 2008R2/2012/2012R2/2016/2019, Apple Mac OS 10.10+, Linux & UNIX
Stacja monitoringu	Obsługa do min. 24 kamer IP (min. 8 darmowych [QVR PRO]).

Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Serwer pocztowy, Stacja monitoringu, Windows ACL, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Replikacja w czasie rzeczywistym, Klient LDAP, Serwer Syslog, Migawki wolumenów, Obsługa kontenerów (LXC – Docker), Serwer VPN
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów
Rozszerzenie	Możliwość rozszerzenia o maksymalnie 16 zatok
Język GUI	Polski, angielski
Gwarancja	Gwarancja minimum 36 miesięcy
Waga	Netto: max 11kg, Brutto: max 17kg
Pobór mocy	Typowy: 69,191W
System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ oraz exFAT
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Liczba kont użytkowników	4096
Liczba grup	512
Liczba udziałów	512
Max ilość połączeń	700
Zasilanie	Redundantne, 2 x 250W
Wentylatory	Minimum 2, o wymiarach co najmniej 70mm
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS
Akcesoria montażowe	W zestawie szyny do montażu w szafie rack

3. **Serwer NAS –** z macierzą do przechowywania plików Urzędu - **1 szt.**

Wymagania ogólne	**W ofercie należy podać nazwę producenta i model** umożliwiające jednoznaczną identyfikację oferowanego produktu.
Procesor	Czterordzeniowy procesor typu ARM o częstotliwości min. 2,2GHz, 64-bitowy, uzyskujący w benchmarku wynik na poziomie przynajmniej 1150 pkt. (https://www.cpubenchmark.net/)"
Obudowa	Rack 3U o wymiarach, 132(H) x 482(W) x 534(D) mm, wraz z kompletem szyn teleskopowych
Ilość slotów RAM	Minimum 2x Long-DIMM DDR4

Pamięć RAM	Minimum 16GB UDIMM DDR4, z możliwością rozbudowy do 32GB
Pamięć Flash	Min. 5000 MB
Ilość obsługiwanych dysków	Min. 16 dysków 2.5"/3.5" SATA3 Hot Swap
Ilość dysków zamontowanych	16 dysków 3,5-cala HDD, min. 10TB SATA, 7200RPM, 256MB cache, min. 1 mln h MTBF, przeznaczony do pracy 24/7, gwarancja producenta min. 3 lata
Interfejsy sieciowe	Minimum 2 x Port 2,5 Gigabit (2,5G/1G/100M), 2 x 10 GbE SFP+
Porty	Min. 1x USB 3.2 Gen 1, 1x USB 3.2 Gen 2, 2x PCIe Gen3 x4
Wskaźniki LED	HDD 1-16, LAN, Power, USB, stan
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0,1,5,5+Spare,6,6+Spare,10,10+Spare,50/60.
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online. Przywracanie RAID.
Szyfrowanie	Możliwość szyfrowania folderów współdzielonych oraz całych woluminów kluczem AES 256 bitów. Mechanizm szyfrowania z akceleracją sprzętową.
Wspierane systemy operacyjne	Windows 7, Windows 8, Windows 10, Windows Server 2008R2/2012/2012R2/2016/2019, Apple Mac OS 10.10+, Linux & UNIX
Stacja monitoringu	Obsługa do min. 24 kamer IP (min. 8 darmowych [QVR PRO]).
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Serwer pocztowy, Stacja monitoringu, Windows ACL, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Replikacja w czasie rzeczywistym, Klient LDAP, Serwer Syslog, Migawki wolumenów, Obsługa kontenerów (LXC – Docker), Serwer VPN
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów
Rozszerzenie	Zainstalowana dwuportowa karta rozszerzeń 10 GbE SFP+ w porcie PCIe
Język GUI	Polski, angielski
Gwarancja	Gwarancja minimum 36 miesięcy
Waga	Netto: max 12kg, Brutto: max 18kg
Pobór mocy	Typowy: 97,34 W
System plików	EXT3, EXT4, NTFS, FAT32, HFS+
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation

Liczba kont użytkowników	4096
Liczba grup	512
Liczba udziałów	512
Max ilość połączeń	700
Zasilanie	Redundantne, 2 x 550W
Wentylatory	Minimum 3, o wymiarach co najmniej 80mm
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS
Akcesoria montażowe	W zestawie szyny do montażu w szafie rack

4. UPS – 18 sztuk

Parametr	Wymagania minimalne
Wymagania ogólne	W ofercie należy podać nazwę producenta i model umożliwiające jednoznaczną identyfikację oferowanego produktu.
Moc pozorna	minimum 650VA
Moc rzeczywista	minimum 360W
Technologia	minimum line-interactive
Typ obudowy	tower
Wejście	
Napięcie wejściowe	minimum 220/230/240 VAC
Zakres napięcia wejściowego	minimum 165-290 VAC
Częstotiwość	minimum 50/60 Hz (auto wykrywanie)
Wyjście	
Regulacja napięcia	minimum '+/- 10 %
Kształt napięcia wyjściowego	minimum symulowana sinusoida
Typowy czas przełączania	2-6 ms
Baterie	
Baterie wewnętrzne w UPS	minimum 12V 7Ah; szczelne, bezobsługowe
Czas podtrzymania (50 % Pmax)	minimum 5 minut
Pozostałe	
Wejście zasilania	kabel zamontowany na stałe w obudowie UPS zakończony wtykiem PL/FR
Ilość i typ gniazd wyjściowych	minimum 2 gniazda Schuko z podtrzymaniem
Stabilizacja napięcia AVR Boost & Buck	wymagana
Filtr RJ45	wymagany

Funkcja autorestartu po powrocie zasilania	wymagana
Funkcja zimnego startu	wymagana
Sygnalizacja	Wyświetlacz LCD, dźwiękowa
Informacje wyświetlane na panelu LCD	minimum napięcie wejściowe i wyjściowe, poziom obciążenia, poziom naładowania baterii, praca z sieci/baterii, przeciążenie, niski poziom baterii
Interfejs komunikacyjny	USB
Zabezpieczenia	minimum przed zwarciem, przeciążeniem, rozładowaniem
Alarmy dźwiękowe	minimum informujące o trybie bateryjnym, rozładowaniu baterii, przeciążeniu, awarii
Waga UPS	do 4,5 kg
Wymiary UPS	nie większe niż: głębokość 290 mm, szerokość 105 mm, wysokość 145 mm
Gwarancja	minimum 24 miesiące na elektronikę i 12 miesięcy na baterie
Serwis	autoryzowany serwis producenta zlokalizowany w Polsce.
	naprawa w maksymalnie 14 dni roboczych
	serwis realizowany w systemie door to door
Oprogramowanie	oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS
	wsparcie dla systemów: Windows, Linux
	wymagane wsparcie producenta w języku polskim (telefoniczne oraz mailowe)
Certyfikaty producenta (załączyć do oferty)	deklaracja zgodności CE
Oświadczenia / dokumenty (załączyć do oferty)	oświadczenie producenta o spełnieniu minimlanych wymaganych parametrów specyfikacji certyfikat lub oświadczenie producenta o posiadaniu przez oferenta statusu Autoryzowanego Partnera - mającego wiedzę w zakresie doboru i sprzedaży zasilaczy UPS

5. Oprogramowanie do zarządzania infrastrukturą

Wymagania ogólne	**W ofercie należy podać nazwę producenta i model oraz wersję** umożliwiające jednoznaczną identyfikację oferowanego oprogramowania.
Ilość licencji	35
Wymagany okres wsparcia technicznego	24 miesiące
Budowa oprogramowania	Oprogramowanie powinno posiadać budowę modułową, składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami powinna być nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. Program powinien umożliwiać zmianę portu

	komunikacyjnego wykorzystywanego przez konsolą zarządzającą. Moduły powinny umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program powinien wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12) i nie może być objęty limitem ilości danych, a baza danych ma być rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających powinna wymagać 64-bitowego systemu operacyjnego Windows.
Wymagania odnośnie polityki zabezpieczenia danych i RODO	Dane, które dotyczą działań pracownika na komputerze (historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp.), powinny być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej i grupowane w osobnym, dedykowanym oknie. Oprogramowanie umożliwiać ma, zgodnie z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty ma być kontrolą na poziomie wybranych Administratorów – program umożliwiać ma nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator ma mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Działania administratorów powinny być logowane, co oznacza, że program powinien posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów powinny być automatycznie eksportowane do zewnętrznego kolektora Syslog.
Polityka haseł	Program powinien umożliwiać konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityka powinna pozwalać na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymuszać dostosowanie bieżących haseł do obowiązujących zasad.
Dwuskładnikowe uwierzytelnienie	Program zawierać powinien mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny powinien być wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA powinno dać się skonfigurować okres, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania powinna być pominięta wyłącznie w lokalnej konsoli serwera.
Jakość zabezpieczeń	Wymaga się, aby producent oprogramowania posiadał znak jakości CYBERSECURITY MADE IN EUROPE, przyznany przez Europejską Organizację ds. Cyberbezpieczeństwa (ECSO).
Monitorowanie	Oprogramowanie powinno mieć możliwość monitorowania infrastruktury bezagentowo, obejmujące serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie: ✓ wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping ✓ wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU) ✓ wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci

	✓ wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki ✓ wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła. ✓ wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku ✓ wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach 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 monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem) - program ma możliwość wykonywania operacji testowych - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa ✓ monitorowania serwerów WWW i adresów URL ✓ cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS ✓ obsługi szyfrowania 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 ✓ monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano ✓ zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny ✓ wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

Zarządzanie	Program powinien posiadać Inteligentne Mapy i Oddziały, służące do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzące dynamiczne mapy wg własnych filtrów (Mapy Inteligentne).
Automatyczne filtrowanie	Kryteria automatycznego filtrowania dotyczyć mają m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program powinien posiadać również funkcję kompilatora plików MIB, umożliwiającego dodawanie definicji dla modułów SNMP.
Alarmy, komunikaty	Program powinien umożliwiać również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy powinny być budowane przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów powinno dać się skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji powinno dać się nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy mają pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie powinno umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0 Program powinien mieć możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).
Inwentaryzacja	- 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 co bezpośrednio będzie umożliwiać audytowanie i weryfikację użytkowania licencji w organizacji. 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 mają być logowane. Moduł inwentaryzacji zasobów powinien umożliwiać ma prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania: ✓ przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, ✓ tworzenia powiązań między zasobami a urządzeniami, ✓ tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych, ✓ wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy, ✓ definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz, ✓ określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, ✓ określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, ✓ definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, ✓ importu danych z zewnętrznego źródła (.CSV), ✓ przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., ✓ tworzenia powiązań między zasobami a dokumentami w relacji 1:N, ✓ oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., ✓ ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, ✓ generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, ✓ przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, ✓ konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, ✓ konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, ✓ archiwizacji i porównywania audytów zasobów, ✓ tworzenia kodów kreskowych dla zasobów,

	✓ drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, ✓ inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet, ✓ możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android, ✓ inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), ✓ definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data" z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja"). 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. 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 i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili powinna być 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.
Obsługa użytkowników	Program 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. Możliwość monitorowania kosztów wydruków, ✓ Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.
Dodatkowe możliwości oprogramowania	Program powinien dodatkowo posiadać możliwość: ✓ wykrywania podejrzanej aktywności przez tzw. „jigglery", mającej na celu symulowanie faktycznej pracy. ✓ zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury. ✓ wyszczególnienia podejrzanej aktywności w raportach. ✓ wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności. ✓ 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 dla użytkownika lub grupy użytkowników i 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. Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji

	powinny być tworzone dla użytkownika lub grupy użytkowników i powinny być kopiowane pomiędzy grupami lub kontami. Program powinien posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.
Zdalna pomoc	W ramach kontroli stacji użytkownika powinien być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania, czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator powinni widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu ma mieć możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu umożliwia równoczesne podłączenie do tego samego komputera kilku administratorom. W niniejszym module ma się znajdywać baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które będą przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie pozwalać ma na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł umożliwiać ma również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach") oraz zawierać dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Oprogramowanie powinno umożliwiać użytkownikom monitorowanie procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, wpisywane i widoczne dla obu stron. System powinien umożliwiać użycie pośredniego statusu „zgłoszenie rozwiązane" przed ostatecznym zamknięciem zgłoszenia. Moduł ten zawierać ma również komunikator (czat), który umożliwiać ma prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto czat powinien pozwalać na: ✓ zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej ✓ rozmowy również między „zwykłymi" użytkownikami ✓ przesyłanie plików między rozmówcami w trybie online ✓ tworzenie pokojów tematycznych, rozmów grupowych ✓ oznaczanie kontaktów jako „ulubionych" na liście kontaktów ✓ uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku ✓ wyświetlanie w trybie jasnym lub ciemnym. W module zawarta ma być również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany,

	wewnętrzny, szkic). Program powinien umożliwiać informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Użytkownik ma mieć możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Dostęp do systemu zgłoszeń oraz bazy wiedzy powinien być realizowany przez dedykowany portal dostępny przez przeglądarkę internetową, wyświetlany w trybie jasnym lub ciemnym. Funkcjonalność modułu powinna umożliwiać również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika. Moduł pomocy zdalnej powinien również umożliwiać: ✓ pobieranie listy użytkowników z Active Directory, ✓ 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, ✓ 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, ✓ 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.
Ochrona danych przed wyciekiem poprzez blokowanie urządzeń	1. Blokowanie urządzeń i nośników danych. Program ma mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. 2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. 3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. 4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane. 5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. 6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender. 7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker. 8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker. 9. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu. 10. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.

	11. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender. 12. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM. Zarządzanie prawami dostępu do urządzeń: 1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. 2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane. 3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. 4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. 5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane. Audyt operacji na plikach na urządzeniach przenośnych: 1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. 2. Podłączenie/odłączenie urządzenia przenośnego. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. Definiowanie reguł monitorowanych folderów w postaci list. Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.) Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych. Program umożliwiać powinien prowadzenie rejestru naruszeń blokad podłączanych nośników.
Zarządzanie czasem i analiza aktywności użytkowników	Program powinien mieć możliwość zarządzania czasem i analizować aktywność użytkowników poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji powinien mieć możliwość oznaczenia sesji aktywności jako czasu prywatnego podczas wykonywania czynności prywatnych na sprzęcie firmowym. Powinien mieć również możliwość uzyskania dostępu do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni mają mieć możliwość uzyskania automatycznego dostępu do aktywności podwładnych w zespołach i indywidualnie oraz możliwość przeanalizowania aktywności w danym okresie i uzyskania pełnego obrazu obszarów wymagających największego zaangażowania. Pracownik powinien posiadać możliwość przeglądania swoich historycznych danych, wybierając okres aktywności, który go interesuje. Zastosowane reguły mają pozwalać zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. Dostęp ma być realizowany przez przeglądarkę internetową, a strona powinna być wyświetlana w trybie jasnym lub ciemnym. 1. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. 2. Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.

	3. Statystyki aktywności podwładnych widoczne dla przełożonego. 4. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem. 5. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu. 6. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników. 7. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych. 8. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. 9. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy. 10. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie). 11. Wskaźnik czasu poświęconego na aktywność produktywną. 12. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail. 13. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji. 14. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów. Portal informacyjny w formie platformy WWW. Oprogramowanie posiadać powinno obszar funkcjonalny w formie platformy WWW, który pozwalać ma na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami. Na każdym z dashboardów widgety powinny być rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych powinna być automatycznie odświeżana oraz: ✓ Udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem. ✓ Wyświetlana w trybie jasnym lub ciemnym (nocnym). Oprogramowanie umożliwiać powinno zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego. Widgety powinny prezentować dane ze wszystkich modułów funkcjonalnych oprogramowania: ✓ Mapa sieci ✓ Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci, ✓ Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów, ✓ Statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW, naruszenia reguł blokad ✓ Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie, ✓ Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem), informacje o stanie Bitlocker, Windows Defender, Windows Firewall, naruszenia reguł dostępu do nośników danych, ✓ Produktywność dla grupy, Statystyki czasu nieproduktywnego.

	Ochrona przed usunięciem. Program powinien być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje. Funkcjonalność Agenta. Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze. Inne. Globalna wyszukiwarka, zwracająca wyniki obiektów różnego typu na podstawie wyszukiwanych słów kluczowych, np.: urządzenia, użytkownicy, zasoby, elementy interfejsu konsoli zarządzającej, elementy opcji. Program ma być dostępny w języku polskim, angielskim, bułgarskim i litewskim, wraz z Podręcznikiem Użytkownika w formie strony internetowej.
Dodatkowe dokumenty	Wymagane jest dołączenie do oferty oświadczenia producenta oprogramowania, że Wykonawca jest oficjalnym partnerem producenta rozwiązania (podać status), a licencje pochodzą z autoryzowanego, oficjalnego kanału – dokumenty potwierdzające należy załączyć do oferty.

6. Serwer wraz z UPS – 2 szt.

Parametr UPSu	Cecha/Wartość/Właściwość
Wymagania ogólne	**W ofercie należy podać nazwę producenta i model** umożliwiające jednoznaczną identyfikację oferowanego produktu.
Minimalne wymagania techniczne dla jednostki UPS	Moc znamionowa jednostki nie mniej niż 1000VA / 700W Obudowa uniwersalna, jednostkę można zainstalować w szafie rack , w zestawie szyny do montażu w szafie rack Technologia Line Interactive Temperatura eksploatacji 0 - 40 °C Wilgotność względna podczas pracy 0 - 95 % Klasa ochrony IP 20 Sprawność urządzenia przy obciążeniu powyżej 80%: min. 98% Klasa energetyczna sprzętu przeciwprzepięciowego minimum 450J
Parametry wejściowe	Nominalne napięcie wejściowe 230V_{AC} Częstotliwość wejściowa 50/60 Hz +/-3 Hz (automatyczne wykrywanie) Typ gniazda wejściowego: - IEC-320 C14 Zakres napięcia wejściowego w trybie podstawowym: 160 - 286V Możliwość zmiany zakresu napięcia
Parametry wyjściowe	Napięcie wyjściowe 230VAC Zniekształcenia napięcia wyjściowego ≤5% Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz ±3 Hz Inne napięcia wyjściowe 220, 240 Typ przebiegu sinusoida, nie dopuszcza się aproksymacji Złącza/gniazda wyjściowe (4) IEC 320 C13 (Zasilanie gwarantowane) 1 programowalna grupa gniazd wyjściowych
Akumulatory i czas podtrzymania	bezobsługowe kwasowo-ołowiowe z elektrolitem w postaci żelu

	Czas autonomii (dla jednostki podstawowej i modułów zewnętrznych): ≥ 8,5 minuty dla pełnego obciążenia ≥ 31 minut dla połowy obciążenia Typowy czas ładowania ≤3 godziny Baterie wewnętrzne wymieniane na gorąco
Komunikacja i zarządzanie	Gniazdo do montażu karty WEB/SNMP- x1 Porty komunikacyjne: RJ45 (port konsoli), USB Możliwość instalacji karty zarządzającej: RJ45 (Ethernet), USB Dodatkowy zainstalowany moduł WEB/SNMP, obsługiwane protokoły komunikacyjne: 1Gb Ethernet IP v.4 i v.6 SNMP v.3 HTTPS/SSL, SSH z kluczem do 2048 bit TLS wersja 1.2 SMTP, NTP, FTP, Telnet Konsola CLI po USB Panel sterowania: Wyświetlacz statusu LED ze wskaźnikiem pracy online: Zasilanie akumulatorowe: Wskaźniki Wymień baterię i Przeciążenie, Wielofunkcyjna konsola sterownicza i informacyjna LCD. Alarm dźwiękowy: Alarm przy zasilaniu akumulatora, alarm przy bardzo niskim poziomie naładowania akumulatora, konfigurowalne opóźnienia. Oprogramowanie do zamykania systemów operacyjnych
Certyfikaty, zgodności oraz gwarancja	CE, EAC, EN/IEC 62040-1, EN/IEC 62040-2 3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulatory

MINIMALNE WYMAGANIA -Serwer	
Uwagi ogólne	**W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu** umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.
Zastosowanie	Serwer baz danych, archiwizacji, wirtualizacji.
Architektura	Obudowa maksymalnie 1U kompatybilna ze standardem szaf rack 19 cali, montowana na szynach, umożliwiającymi serwisowanie serwera w szafie bez wyłączania urządzenia. Obudowa z możliwością instalacji do 8 dysków 2.5" Hot-Plug.
Procesor	Zainstalowany jeden procesor 16-rdzeniowy, min. 2.4 GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 28.500 w teście Average CPU Mark - Multithread Rating dostępnym na stronie https://www.cpubenchmark.net/. lub opublikowanym w dniu 19.08.2024.
Płyta główna	Płyta główna dedykowana do pracy w serwerach, zaprojektowana i wyprodukowana przez producenta serwera. Płyta główna zapewnia możliwość pracy 2 procesorów po minimum 24 rdzeni każdy. Płyta główna musi posiadać przynajmniej 16 slotów pamięci RAM typu DDR4 umożliwiających rozszerzenie pamięci do maksymalnie 1TB.
Pamięć RAM	Nie mniej niż 128GB pamięci DDR4 RDIMM, w minimum 4 kościach w celu zwiększenia wydajności oferowanego rozwiązania.
Karty HBA/NIC/PCIe	Zainstalowany sprzętowy kontroler dysków SAS/SATA z 8GB cache z podtrzymaniem oraz funkcjonalnością RAID 0,1,10,5,6,50,60.

	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy 10Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez zainstalowanie karty w wymaganych slotach PCIe).
Zamontowane dyski twarde	Min. 4 szt. jednakowych dysków Hot-Plug SATA3 SSD o pojemności minimum 960GB każdy. Konfiguracja RAID 5. Możliwość zainstalowania karty obsługującej co najmniej dwa dyski M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Karta graficzna	2D, zintegrowana z płytą główną.
Zewnętrzne porty wejścia / wyjścia	Przód obudowy co najmniej: 1 port USB 3.0; 1 port Video VGA; 1 port USB – dedykowany do zarządzania Tył obudowy co najmniej: 1 port USB 3.0; 1 port USB 2.0; 1 port Video VGA; 1 port RJ45 dedykowany do zarządzania
Zdalne zarządzanie	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
Diagnostyka	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Zasilanie	2 zasilacze nadmiarowe o mocy co najmniej 700W każdy, technologia Hot-Plug. W zestawie kable zasilające złącza C14 IEC320 o długości min. 1.8m.

System operacyjny	Dostarczony system operacyjny przez wzgląd na kompatybilność z obecnie posiadaną infrastrukturą. Licencja na Windows Server 2022 Standard, licencja pokrywająca wszystkie fizyczne rdzenie w serwerze. System zainstalowany na wymaganych nośnikach, preinstalowana partycja recovery.
Bezpieczeństwo	Zatrzask górnej pokrywy oraz blokada na ramce panelu, zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Wspierane systemy operacyjne	- Canonical® Ubuntu® Server LTS. - Citrix® Hypervisor. - Microsoft Windows Server® z technologią Hyper-V. - Red Hat® Enterprise Linux. - SUSE® Linux Enterprise Server. - VMware® ESXi.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów x64, Microsoft Windows Server 2022, Microsoft Windows Server 2019.
Gwarancja	1. Serwis gwarancyjny producenta realizowany przez okres 3 lat od daty zakupu, świadczony w miejscu użytkowania serwera, obejmujący wszystkie komponenty serwera. 2. Możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 3. Czas reakcji autoryzowanego serwisu producenta: od dnia zgłoszenia awarii do końca następnego dnia roboczego. 4. W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. 5. Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera.
Dokumentacja, inne	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. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

	Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
Akcesoria montażowe	W zestawie szyny do montażu w szafie rack

7. Przełącznik sieciowy – 10 szt.

Klasa przełącznika	SMART
Typ obudowy	Rack
Warstwa przełączania	L2
Architektura sieci	GigabitEthernet
Liczba portów 10/100/1000 Mbps	Minimum 8 szt.
Liczba portów PoE (PoE + PoE+):	Minimum 8 szt.
Liczba portów SFP	Minimum 2 szt.
Tryb przekazywania	Store-and-forward
Przepustowość	20 Gb/s
Prędkość przekazywania	14.9 Mpp
Bufor pakietów	512 KB
Rozmiar tablicy adresów MAC	8192
Obsługa ramek Jumbo	Tak
Rozmiar ramki Jumbo	9 KB
VLAN	Minimum obsługa protokołu IEEE802.1Q, do 512 grup VLAN oraz 4096 identyfikatorów VID
Obsługiwane protokoły i standardy	Minimum IEEE 802.3i, IEEE 802.3u, IEEE 802.3z, IEEE 802.3ab, IEEE 802.3ad, IEE 802.3af, IEEE 802.3x, IEEE 802.1d, IEEE 802.1s, IEEE 802.1w, IEEE 802.1q, IEEE 802.1p
QoS	Obsługa priorytetowania 802.1p CoS/DSCP - Obsługa 4 kolejek priorytetowania - Harmonogram kolejek: SP, WRR, SP+WRR - Ograniczanie prędkości transferu w oparciu o port/przepływ danych - VLAN Voice
Bezpieczeństwo	SSH v1/v2 - SSL v2/v3/TLSv1 - Port Security - Broadcast/Multicast/Unknown-unicast Storm Control
Zarządzanie, monitorowanie, konfiguracja	Interfejs przeglądarki internetowej GUI, interfejs linii poleceń CLI - SNMP v1/v2c/v3, zgodne z publicznymi bibliotekami MIB i prywatnymi bibliotekami MIB TP-LINK - RMON (grupy 1, 2, 3, 9) - Monitorowanie CPU - Port Mirroring - Automatyczne ustawianie czasu: SNTP - Aktualizacja firmware: poprzez przeglądarkę internetową oraz TFTP - Diagnostyka: test VCT - Logi systemu, publiczne biblioteki MIB
Funkcje L2	IGMP Snooping V1/V2/V3 - Agregacja portów - LACP (Do 6 grup agregacji obejmujących do 4 portów każda) - STP/RSTP/MSTP -

	Filtrowanie/ochrona BPDU - Ochrona TC/Root - Wykrywanie połączeń loopback - Kontrola przepływu 802.3x - LLDP(LLDP-MED
Pobór mocy	8.5 W
Akcesoria w zestawie	Zasilacz - Instrukcja instalacji - Płyta CD - Gumowe nóżki
Zasilanie	100~240VAC, 50/60Hz
Wymiary	209 x 126 x 26mm
Maksymalna moc całkowita podłączonych urządzeń	Do 53W

Część II – szkolenia

1. Szkolenia mają obejmować:
    1) Zarzadzanie Windows Serwer, usługą katalogową pod kątem cyberbezpieczeństwa,
    2) Zarządzanie oraz konfiguracja serwerów plików NAS,
    3) Zaawansowana konfiguracja aplikacji do tworzenia kopii zapasowych,
    4) Szkolenie z aplikacji do zarządzania infrastrukturą IT
2. Szkolenie z obsługi wyspecyfikowanego w cz. I opisu przedmiotu zamówienia serwera NAS – wymagania minimalne:
    a) Wykonawca zapewni certyfikowane szkolenie (online, min. 7 godzin) dla administratora Zamawiającego (1 osoba) z obsługi rozwiązania sprzętowego do tworzenia kopii zapasowych i ich odzyskiwania prowadzone przez trenera posiadającego autoryzację producenta na prowadzenie szkolenia z dostarczonego rozwiązania.
    b) udzielenie zamówienia mogą się ubiegać Wykonawcy, którzy posiadają zdolności techniczne lub zawodowe. Wykonawca spełnia w/w warunek jeżeli wykaże, że trener prowadzący szkolenie posiada co najmniej jeden certyfikat techniczny producenta
    c) Szkolenie musi zawierać min. poniższe zagadnienia:
    przegląd portfolio produktowego producenta NASa; podstawowe informacje o możliwościach sprzętowych i programowych; zarządzanie dyskami i konfiguracja przestrzeni; konfiguracja użytkowników i grup; architektura przestrzeni dyskowej ; dobór dysków twardych i możliwości konfiguracji; konfiguracja puli pamięci oraz grup RAID; konfiguracja woluminów; konfiguracja iSCSI LUN; konfiguracja SSD cache; VJBOD / VJBOD cloud; cacheMount; przechowywanie danych; zarządzanie uprawnieniami; tworzenie folderów udostępnionychudziały sieciowe; backup i replikacja; backup hybrydowy; deduplikacja; wirtualizacja; konfiguracja sieci wirtualnej; wirtualizacja; kontenery; zabezpieczenie; zabezpieczenie przed atakami brute force; konfiguracja antywirusa; szyfrowanie dysków i katalogów; zarządzanie hasłami użytkowników; weryfikacja poprawności działania urządzenia.
3. Szkolenie z obsługi serwerowego systemu operacyjnego firmy Microsoft
    a) Wykonawca zapewni certyfikowane szkolenie (online, min. 16 godzin, powinno zostać zrealizowane w ciągu maksymalnie 3 dni) dla administratora Zamawiającego (1 osoba) z obsługi rozwiązania sprzętowego do tworzenia kopii zapasowych i ich odzyskiwania prowadzone przez trenera posiadającego autoryzację producenta na prowadzenie szkolenia z dostarczonego rozwiązania.
    b) udzielenie zamówienia mogą się ubiegać Wykonawcy, którzy posiadają zdolności techniczne lub zawodowe. Wykonawca spełnia w/w warunek jeżeli wykaże, że trener prowadzący szkolenie posiada certyfikat: Microsoft Certified Trainer.
    Wykonawca udostępni na czas trwania szkolenia odpowiednie oprogramowanie niezbędne

do wykonywania ćwiczeń praktycznych podczas szkolenia oraz zapewni minimum 14-dniowy kontakt mailowy z trenerem po zrealizowanym szkoleniu.

c) Szkolenie musi zawierać min. poniższe zagadnienia: instalacja i konfiguracja kontrolerów domeny, zarządzanie obiektami w AD DS., zarządzanie zaawansowaną infrastrukturą AD DS., wdrażanie i zarządzanie lokacjami i repliką AD DS., wdrażanie zasad grupy, zarządzanie ustawieniami użytkowników za pomocą zasad grupy

4. Szkolenie z obsługi posiadanego przez Zamawiającego oprogramowania do backupu - Acronis Cyber Protect - Backup Standard Workstation
   a) Wykonawca zapewni szkolenie (online, min. 7 godzin) dla administratora Zamawiającego (1 osoba) z rozwiązanie do tworzenia kopii zapasowych i ich odzyskiwania.
   b) Szkolenie ma się odbywać w formie online, ma być poprowadzone przez trenera posiadającego autoryzację producenta na prowadzenie szkolenia z dostarczonego rozwiązania.
   c) Szkolenie musi zawierać min. poniższe zagadnienia: omówienie konsoli do zarządzania, instalacja agentów, sposoby aktualizacji agentów, tworzenie planów kopii zapasowej, tworzenie planu backupu całego systemu oraz baz SQL, weryfikacja kopii zapasowej, odzyskiwanie kopii zapasowej, tworzenie i zastosowanie nośnika startowego.
5. Szkolenie z aplikacji do zarządzania infrastrukturą IT opisaną w cz. I opisu przedmiotu zamówienia
   a) Wykonawca zapewni certyfikowane szkolenie (online, min. 2 dniowe) dla administratora Zamawiającego (1 osoba) z obsługi oprogramowania do zarządzania infrastrukturą wyspecyfikowanego w cz. I opisu przedmiotu zamówienia
   b) udzielenie zamówienia mogą się ubiegać Wykonawcy, którzy posiadają zdolności techniczne lub zawodowe. Wykonawca spełnia w/w warunek jeżeli wykaże, że trener prowadzący szkolenie posiada co najmniej jeden certyfikat techniczny producenta.
   c) Szkolenie musi zawierać min. poniższe zagadnienia:
   Omówienie interfejsu użytkownika; monitorowanie urządzeń i sieci; tworzenie i edytowanie raportów podstawowych (wykresy, tabele, analiza danych); podstawowe funkcje analityczne i zarządzanie zasobami; prezentowanie danych w formie raportów i alertów; instalacja i konfiguracja oprogramowania; zarządzanie licencjami, użytkownikami i uprawnieniami; monitorowanie systemu i zapewnianie jego stabilności; podstawy rozwiązywania problemów i wsparcie techniczne; aktualizacje systemu i zarządzanie wersjami oprogramowania.