|  |  |
| --- | --- |
| **OPIS PRZEDMIOTU ZAMÓWIENIA**  Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja z przeprowadzeniem szkolenia.  **Przedmiot zamówienia obejmuje niżej wymieniony asortyment.** | |
| **Cecha/Funkcjonalność** | **Minimalne parametry wymagane przez Zamawiającego** |
| **Oprogramowanie antywirusowe – 50szt.** | |
| **Konsola zarządzająca** | Konsola web administratora powinna znajdować się w chmurze producenta  znajdującej się na terenie Unii Europejskiej i zapewniać możliwość pełnego zarządzania stacjami roboczymi/serwerami przez przeglądarkę Web, która ma dostęp do Internetu.  Konsola web administratora musi posiadać możliwość wyboru języka polskiego.  Konsola web musi umożliwiać zarządzanie stacjami roboczymi oraz serwerami i urządzeniami mobilnymi poprzez tą samą konsolę zarządzającą.  Konsola web musi posiadać możliwość tworzenia grup i polityk dla stacji.  Administrator musi mieć możliwość przenoszenia licencji pomiędzy urządzeniami stacjonarnymi i odrębnie między urządzeniami mobilnymi  Administrator musi mieć możliwość zarządzania kluczem licencyjnym z poziomu konsoli administracyjnej.  Konsola web musi umożliwiać bezpieczne logowanie do konsoli zarządzającej po protokole HTTPS z certyfikatem.  Konsola web musi umożliwiać dwuetapową autoryzację logowania na minimum 2 sposoby.  Konsola web musi posiadać możliwość zablokowania dostępu do ustawień programu ochrony dla użytkowników na urządzeniach nieposiadających uprawnień administracyjnych.  Konsola web musi posiadać funkcję, która uniemożliwia użytkownikowi komputera wyłączenie działania monitora antywirusowego i innych składników ochrony, jeżeli nie posiada uprawnień administratora.  Konsola web musi posiadać narzędzie do wykonania instalacji oprogramowania na stacjach poprzez Active Directory, grupy robocze lub zakresy adresów sieciowych IP.  Konsola web musi umożliwiać wykonanie instalacji oprogramowania firm trzecich zdalnie z konsoli na stacjach bezpośrednio z bezpiecznego repozytorium dostawcy rozwiązania antywirusowego.  Konsola web musi mieć możliwość zalogowania się kilku administratorom jednocześnie.  Konsola web powinna oferować predefiniowane domyślne ustawienia rekomendowanych polityk (ustawień) dla stacji końcowych.  Konsola web umożliwia zmianę ustawień priorytetu skanowania.  Konsola web musi mieć funkcję planowania zadań, w tym planowania terminów automatycznego skanowania.  Konsola web umożliwia wysyłanie powiadomień o zdarzeniach na wskazany adres mailowy.  Konsola web musi posiadać możliwość uruchamiania komputerów zdalnie (WakeOnLAN), uruchamiania ponownego oraz wyłączania urządzeń z systemem Windows.  Konsola web musi umożliwiać synchronizację z Azure Active Directory.  Konsola web musi obsługiwać moduł do odbierania zgłoszeń serwisowych od użytkowników bezpośrednio z aplikacji zainstalowanej na stacji klienckiej.  Rozwiązanie musi posiadać dedykowaną aplikację lub stronę internetową do zgłoszeń serwisowych bez konieczności instalacji ochrony antywirusowej.  Konsola web musi posiadać zintegrowany moduł CRM z możliwością zaplanowania prac u użytkownika.  Konsola web musi posiadać moduł uruchamiania procedur (skrypty) zdefiniowanych przez producenta oraz przez użytkownika w języku Python lub JSON.  Oprogramowanie web musi zawierać zintegrowaną funkcjonalność menadżera aktualizacji (Patch Manager), który umożliwia zarządzanie pobieraniem aktualizacji (updatów) systemu Windows, Java, Adobe i innych producentów trzecich.  Producent powinien posiadać własne bezpieczne i sprawdzone repozytorium aplikacji do celów aktualizacji oprogramowania firm trzecich minimum 50 producentów |
| **Zarządzanie użytkownikami i stacjami** | Rozwiązanie musi umożliwiać bezpośrednio z konsoli zarządzającej web uruchamianie procedur (skryptów) serwisowych na stacjach klienckich o minimalnych, następujących funkcjonalnościach:  Czyszczenie plików tymczasowych  Czyszczenie i sprawdzanie dysku  Usuwanie błędów dysku  Defragmentowanie dysku  Czyszczenie kolejki drukarki  Czyszczenie pamięci podręcznej DNS  Czyszczenie kosza  Sprawdzanie błędów na dysku twardym S.M.A.R.T. Check  Włączenie szyfrowania dysku funkcją Bitlocker dla systemu Windows  System powinien przyjmować zgłoszenia serwisowe bezpośrednio z agenta na stacji, pocztą email oraz po przez dedykowaną stronę dla działu serwisu.  System musi umożliwiać przydzielanie zgłoszenia serwisowego dla konkretnego administratora oraz powinien mieć zintegrowany system diagnozy stacji oraz możliwość podłączenia się poprzez zdalny pulpit.  Konsola web musi posiadać zintegrowany moduł umożliwiający zdalne połączenie z graficznym pulpitem zdalnym przez dedykowaną aplikację dla komputerów/serwerów znajdujących się w sieci LAN i poza nią bez potrzeby tworzenia tuneli VPN każdej stacji komputera/serwera/Windows.  Możliwość wyświetlania komunikatu przed połączeniem zdalnym pulpitem do użytkowania przez administratora w określonym przez niego czasie.  Możliwość wyświetlania komunikatu przed połączeniem zdalnym pulpitem do użytkowania przez administratora w celu odpytania go o zgodę na połączenie.  Konsola web musi mieć funkcję tworzenia raportów o stacjach w konsoli.  Konsola web musi mieć funkcję logów wykonywanych czynności przez administratorów konsoli. |
| **Agent ochrony konsoli – oprogramowanie antywirusowe** | Program antywirusowy musi mieć obsługę w języku polskim. Platforma powinna obsługiwać m.in. systemy operacyjne:  macOS:  10.14.x  10.15.x  11.x  12.x  13.x  14.x  MS Windows (stacje klienckie):  Windows XP (SP3 or higher) x86  Windows 7 SP1 x86  Windows 7 SP1 x64  Windows 8 x86  Windows 8 x64  Windows 8.1 x86  Windows 8.1 x64  Windows 10 x86  Windows 10 x64  Windows 11 x64  MS Windows (wersja serwerowa):  Windows Server 2003 SP2  Windows Server 2003 R2 SP2  Windows Server 2008 SP2  Windows Server 2008 R2  Windows Server 2012  Windows Server 2012 R2  Windows Server 2016  Windows Server 2019  Windows Server 2022  LinuxOS z gwarantowaną kompatybilnością:  Latest Ubuntu 16.х LTS x64 release version (with GUI)  Latest Ubuntu 18.х LTS x64 release version (with GUI)  Latest Ubuntu 19.х x64 release version (with GUI)  Latest Ubuntu 20.х LTS x64 release version (with GUI)  Latest Ubuntu 21.04 x64 release version (with GUI)  Latest Debian 8.х x64 release version (with GUI)  Latest Debian 9.x x64 release version (with GUI)  Latest Debian 10.x x64 release version (with GUI)  Latest Red Hat Enterprise Linux Server 7.х x64 release version (with GUI)  Latest Red Hat Enterprise Linux Server 8.х x64 release version (with GUI)  Latest CentOS 7.х x64 release version (with GUI)  Latest CentOS 8.х x64 release version (with GUI)  Rozwiązanie powinno działać na komputerach wyposażonych minimalnie w:  512 MB dostępnej pamięci RAM  1 GB miejsca na dysku twardym dla wersji 32-bitowej i 64-bitowej  Instalacja oprogramowania musi być możliwa poprzez Active Directory, grupy robocze, poprzez sieć, pobranie paczki MSI i za pomocą dystrybucji przez pocztę e-mail.  Oprogramowanie powinno mieć możliwość przeglądania obciążenia procesów na stacji i serwerze oraz zawartości dysków z poziomu konsoli web.  Ochrona poczty - antywirus musi chronić stacje poprzez uruchamianie nieznanych oraz niebezpiecznych załączników w środowisku wirtualnym na stacji takim jak lokalna i automatyczna piaskownica (auto-sandbox).  Oprogramowanie umożliwia funkcję chat między administratorem konsoli a stacjami roboczymi (windows)  Program antywirusowy musi posiadać możliwość skanowania wybranych plików, folderów/katalogów (również skompresowanych), a także całych dysków (w tym sieciowych) czy partycji.  Oprogramowanie umożliwia cykliczne zrzuty ekranu podpiętych do konsoli stacji.  Oprogramowanie umożliwia w konsoli WEB na:  1. Podgląd uruchomionych procesów na danej stacji oraz ich zamknięcie  2. Przeglądanie plików stacji końcowej  3. Podgląd uruchomionych usług oraz ich restart i zakończenie  4. Wykonywanie poleceń CMD i Powershell w przeglądarce  5. Podgląd systemowego dziennika zdarzeń  Oprogramowanie umożliwia pełną wizualną personalizację aplikacji.  Oprogramowanie umożliwia przypisanie aplikacji z repozytorium udostępnionego przez producenta  Oprogramowanie umożliwia na rejestrowanie lokalne wszystkich zdarzeń z aplikacji oraz wysyłanie ich na zewnętrzny serwer SYSLOG  Oprogramowanie umożliwia monitorowanie:  Monitorowanie wydajności pracy: CPU, RAM, sieci, dysku  Rozmiaru plików i folderów  Pojemności dysku  Aktywnych procesów  Podgląd dziennika zdarzeń systemu  Aktywnych połączeń sieciowych  Stron WWW  Zdarzeń aktualizacji systemu operacyjnego  Program antywirusowy musi posiadać możliwość skanowania dowolnego zasobu podłączonego do stacji roboczej np.: dyski zewnętrzne, pamięci USB  Program antywirusowy powinien posiadać filtering URL umożliwiający blokowanie konkretnych stron internetowych.  Program antywirusowy musi posiadać moduł antywirusowy chroniący w czasie rzeczywistym.  Program antywirusowy musi posiadać moduł sprawdzający reputację plików w chmurze.  Program antywirusowy musi posiadać dwukierunkowy konfigurowalny z konsoli web firewall z możliwością tworzenia polityk globalnych i z podziałem na aplikacje.  Program antywirusowy musi posiadać moduł HIPS (Host Intrusion Protection System – ochrona antywłamaniowa).  Program antywirusowy musi posiadać moduł automatycznej piaskownicy (autosandbox), odizolowanego środowiska wirtualnego, w którym zasoby są emulowane dla obiektów w nim umieszczonych. Dodatkowo cały proces izolacji dzięki temu modułowi musi odbywać się lokalnie, na stacji roboczej. Całe środowisko wirtualne musi być odwzorowaniem 1:1 z systemem operacyjnym. Użytkownik powinien móc pracować w zwirtualizowanym środowisku, bez możliwości zapisu na stacji poza środowiskiem wirtualnym.  Program antywirusowy musi posiadać możliwość uruchomienia dowolnego pliku/programu w automatycznej piaskownicy (auto-sandbox) na żądanie użytkownika (manualnie).  Program antywirusowy musi umożliwiać użytkownikowi wysłanie podejrzanego obiektu do producenta oprogramowania antywirusowego w celu jego analizy. Funkcja ta powinna być dostępna z interfejsu programu antywirusowego.  Podczas pracy komputera Program musi automatycznie skanować:  pliki uruchamiane, otwierane,  pliki kopiowane lub przenoszone,  pliki tworzone,  pliki pobierane z Internetu po protokole HTTP/HTTPS.  W przypadku wykrycia wirusa program musi posiadać możliwość automatycznego poddawania kwarantannie podejrzanych obiektów oraz opcję przywrócenia z kwarantanny usuniętych obiektów.  Program antywirusowy musi posiadać funkcję dodawania wyjątków do modułu antywirusowego, automatycznej piaskownicy (auto-sandbox) czy modułu HIPS.  Program antywirusowy powinien posiadać dodatkowe narzędzie do skanowania systemu.  Program antywirusowy musi posiadać dodatkowe narzędzie do analizowania  bezpieczeństwa procesów.  Program antywirusowy powinien mieć możliwość skanowania skompresowanych plików.  Program antywirusowy musi być z możliwością zablokowania dostępu do zmiany ustawień programu hasłem administratora oraz hasłem skonfigurowanym w konsoli zarządzającej.  Program antywirusowy powinien mieć możliwość importowania oraz eksportowania ustawień.  Program antywirusowy powinien mieć możliwość tworzenia list zaufanych procesów.  Program antywirusowy powinien mieć możliwość tworzenia list zaufanych plików.  Program antywirusowy i konsola powinny umożliwiać tworzenie wyjątków ze skanowania folderów / plików.  Program antywirusowy powinien umożliwiać konfigurację polityk (globalnych ustawień dla grup endpoint'ów) w celu szybkiej implementacji ustawień bezpieczeństwa dla wielu urządzeń.  Program antywirusowy powinien umożliwiać zmianę ustawień priorytetu skanowania.  Program antywirusowy powinien umożliwiać skanowanie pamięci komputera po uruchomieniu.  Program antywirusowy posiada zintegrowaną funkcję skanowania i ochrony plików pod kątem danych wrażliwych (DLP).  Program antywirusowy posiada zintegrowaną funkcję blokowania urządzeń  zewnętrznych / przenośnych przed odczytem, edycją i zapisem plików w tym samym czasie.  Program antywirusowy posiada zintegrowaną funkcję blokowania jedynie zapisu plików na urządzeniach zewnętrznych / przenośnych.  Program antywirusowy powinien posiadać możliwość aktualizowania baz danych antywirusowych ręcznie, nawet jeśli komputer nie będzie miał dostępu do Internetu.  Program antywirusowy musi posiadać zintegrowane środowisko, dzięki któremu możemy bezpiecznie działać w wirtualnym systemie nawet na zainfekowanej stacji. Środowisko to musi być odizolowanie od reszty systemu operacyjnego i mieć możliwość uruchomienia takich sesji bez wprowadzonych wcześniejszych zmian przez użytkownika w tym narzędziu (czyste środowisko). Ma również pozwalać na bezpieczniejsze wykonywanie przelewów bankowych, bez obaw, że system operacyjny, na którym działa dany komputer nie został uprzednio zmodyfikowany i byłby w stanie zagrozić utracie np. danych logowania do kont bankowych.  Oprogramowanie powinno mieć możliwość przeglądania obciążenia procesów na stacji i serwerze oraz zawartości dysków z poziomu konsoli web.  Oprogramowanie umożliwia funkcję chat między administratorem konsoli a stacjami roboczymi (Windows).  Oprogramowanie chroni przed nieupoważnionym zrzutem obrazu z ekranu.  Oprogramowanie umożliwia analizę skryptu w programach pod kątem złośliwego oprogramowania przed ich uruchomieniem.  Oprogramowanie umożliwia na rejestrowanie dzienników zdarzeń oraz zapisywanie ich lokalnie i na zewnętrznym serwerze.  Oprogramowanie umożliwia personalizację wyglądu agenta ochrony.  Oprogramowanie umożliwia zastosowanie proxy do rozpropagowania aktualizacji wewnątrz sieci.  Oprogramowanie umożliwia procentową regulację zużycia zasobów procesora oraz nadania priorytetu.  Oprogramowanie umożliwia śledzenie bibliotek uruchomionych przez procesy oraz blokowanie nieznanych bibliotek |
| **Dodatkowe systemy bezpieczeństwa** | Konsola web musi posiadać możliwość śledzenia historii zagrożeń na wybranych komputerach.  Konsola web musi posiadać moduł zapobiegania wyciekowi danych DLP możliwością włączenia skanowania plików w wybranych lokalizacjach na komputerach pod kątem znajdujących się w nich danych wrażliwych przez zdefiniowane wzory z możliwością dodawania własnych reguł DLP oraz powinna umożliwiać sprawdzenia logów z tej czynności.  Konsola web zintegrowana z wszystkimi poprzednimi modułami i funkcjami musi umożliwić przeprowadzenia skanowania sieci firmowej (również za pomocą protokołu SNMP) w celu przeprowadzenia audytu urządzeń działających w tej sieci. |
| **Moduł detekcji zagrożeń na urządzeniach końcowych** | Rozwiązanie zawiera w sobie moduł oparty na technologii typu "Endpoint Detection & Response", zwany dalej EDR.  Moduł EDR ma funkcję śledzenia zdarzeń systemowych i sieciowych urządzeń na których jest wdrożony.  Moduł EDR ma funkcję alertowania wybranych zdarzeń, typowanych na stanowiące potencjalne zagrożenie dla cyberbezpieczeństwa, zgodnie z przyjętą polityką.  Polityka bezpieczeństwa musi być edytowalna i mieć możliwość wprowadzania samodzielnie zdefiniowanych reguł. Nie jest dopuszczalne ograniczenie do reguł predefiniowanych przez producenta.  Funkcja śledzenia zdarzeń musi mieć możliwość ich filtrowania względem co najmniej 10-ciu parametrów, w szczególności:  a) urządzenia  b) użytkownika  c) podsystemu bezpieczeństwa  d) techniki potencjalnego ataku.  e) taktyki potencjalnego ataku.  Moduł EDR musi mieć możliwość korelacji ewentualnych powiązań pomiędzy śledzonymi zdarzeniami i przedstawienia ich z użyciem sygnatur czasowych i/lub na osi czasu.  Korelacja zdarzeń śledzonych przez EDR ma dotyczyć w szczególności:  a) zmian w plikach  b) zmian w rejestrze systemowym  c) działających procesów i podprocesów  d) dostępu do urządzeń zewnętrznych |
| **Urządzenia mobilne** | Konsola zarządzająca  Konsola web administratora powinna znajdować się w chmurze producenta  znajdującej się na terenie Unii Europejskiej i zapewniać możliwość pełnego zarządzania stacjami roboczymi/serwerami przez przeglądarkę Web, która ma dostęp do Internetu.  Konsola web administratora musi posiadać możliwość wyboru języka polskiego.  Konsola web musi umożliwiać zarządzanie urządzeniami mobilnymi poprzez tę samą konsolę zarządzającą.  Konsola web musi posiadać możliwość tworzenia grup i polityk dla urządzeń mobilnych.  Administrator musi mieć możliwość przeniesienia z poziomu konsoli aktywnej licencji na inne urządzenie mobilne bez utraty ważności licencji.  Administrator musi mieć możliwość zarządzania kluczem licencyjnym z poziomu konsoli administracyjnej.  Konsola web musi umożliwiać bezpieczne logowanie do konsoli zarządzającej po protokole HTTPS z certyfikatem.  Konsola web musi umożliwiać dwuetapową autoryzację logowania na minimum 2 sposoby.  Konsola web musi umożliwiać wykonanie instalacji oprogramowania firm trzecich zdalnie z konsoli na urządzeniach mobilnych.  Konsola web musi umożliwiać geolokalizację z aktualną mapą urządzeń mobilnych iOS/Android wyposażonych w moduł GPS.  Konsola web musi mieć możliwość zdefiniowana zalecanych aplikacji, które może pobrać użytkownik urządzeń mobilnych.  Konsola web umożliwia zdalną deinstalację jak i blokadę aplikacji firm trzecich na urządzeniu mobilnym  Konsola web musi umożliwiać wyczyszczenie lub zablokowanie zdalne urządzenia mobilnego.  Konsola web musi mieć możliwość zalogowania się kilku administratorom jednocześnie.  Konsola web powinna oferować predefiniowane domyślne ustawienia rekomendowanych polityk (ustawień) dla urządzeń mobilnych  Konsola web musi mieć funkcję planowania zadań, w tym planowania terminów automatycznego skanowania.  Konsola web musi obsługiwać moduł do odbierania zgłoszeń serwisowych od użytkowników bezpośrednio z urządzenia mobilnego.  Rozwiązanie musi posiadać dedykowaną aplikację lub stronę internetową do zgłoszeń serwisowych bez konieczności instalacji ochrony antywirusowej.  Konsola web musi mieć funkcję tworzenia raportów o urządzeniach mobilnych w konsoli.  Konsola web musi mieć funkcję logów wykonywanych czynności przez administratorów konsoli.  Konsola i oprogramowanie umożliwia w szczególności:  Włączenie/Wyłączenie syreny na urządzeniu mobilnym  Wysłanie komunikatu do urządzenia mobilnego  Zmianę kodu dostępu  Blokowanie/Odblokowanie aplikacji oraz ich deinstalację  Zdjęcie z przedniej kamery w przypadku przekroczenia ilości prób logowania  Aktualizacja lokalizacji urządzenia mobilnego  Całkowite wyczyszczenia urządzenia  Blokada urządzenia  Zmiana hasła dostępu  Wspiera funkcję ActiveSync  Użyj szyfrowania serwera poczty przychodzącej (SSL)  Akceptuj wszystkie certyfikaty (dla poczty przychodzącej)  Zaakceptuj certyfikaty TLS (dla poczty przychodzącej)  korzystanie z certyfikatu  Zabroń przemieszczania poczty na inne konta  Tryb Kiosk dla urządzeń  Konfigurację min. VPN (L2TP/PPTP/L2TP IPSEC PSK/IPSEC XAUTH PSK/IPSEC XAUTH RSA)  Oprogramowanie umożliwia ograniczenia korzystania z Bluetooth  Zezwalaj/Zablokuj na wykrywanie urządzeń przez Bluetooth  Pozwól/Zablokuj na parowanie urządzenia Bluetooth  Zezwalaj/Zablokuj na połączenia wychodzące  Zezwól/Zablokuj na Tethering przez Bluetooth  Zezwalaj/Zablokuj na połączenie z komputerem stacjonarnym lub laptopem przez Bluetooth  Zezwalaj/Zablokuj na przesyłanie danych  Oprogramowanie umożliwia ograniczenia korzystania z przeglądarki  Zezwalaj/Zablokuj na wyskakujące okienka  Pozwól/Zablokuj korzystać z JavaScript  Akceptuje/Zablokuj ciasteczka  Zapamiętaj/Zablokuj dane formularza do późniejszego wykorzystania  Pokaż/Zablokuj ustawienia ostrzeżeń o oszustwach  Oprogramowanie umożliwia ograniczenia korzystania z aplikacji  Zezwól/Zablokuj na korzystanie z Gmaila  Zezwól/Zablokuj na korzystanie z poczty e-mail  Zezwól/Zablokuj na korzystanie z przeglądarki  Zezwól/Zablokuj na korzystanie z galerii  Zezwól/Zablokuj na Google Play  Zezwól/Zablokuj na korzystanie z aplikacji YouTube  Zezwól/Zablokuj na Mapy Google i nawigację Google  Zezwól/Zablokuj na wyszukiwanie Google i głosowe  Zezwól/Zablokuj Chrome Browser  Zezwól/Zablokuj Galaxy Store  Oprogramowanie umożliwia ograniczenia sieciowe  Zezwól/Zablokuj tylko na połączenia alarmowe  Zezwól/Zablokuj na roaming głosowy  Zezwól/Zablokuj na synchronizację podczas roamingu  Zezwól/Zablokuj na roaming danych  Zezwól/Zablokuj na tethering przez USB  Zezwól/Zablokuj na zmianę ustawień punktu dostępu Wi-Fi  Zezwól/Zablokujj użytkownikowi na dodawanie sieci Wi-Fi  Minimalny poziom bezpieczeństwa sieci Wi-Fi  -Otwarta  -WEP  -WPA  -802.1.x EAP(FAST/LEAP/PEAP/TTLS/TLS)  Zezwól/Zablokuj na korzystanie z SMS-ów  Zezwól/Zablokuj na korzystanie z MMS  SSID na czarnej liście  Oprogramowanie ogranicza w szczególności:  Zezwól/Zablokuj na połączenie z USB  Zezwól/Zablokuj użyj czasu sieciowego  Zezwól/Zablokuj korzystać z mikrofonu  Zezwól/Zablokuj na Near Field Communication (NFC)  Zezwól/Zablokuj na fałszywe lokalizacje  Zezwól/Zablokuj na dostęp do karty SD  Zezwól/Zablokuj na zapis na karcie SD  Zezwól/Zablokuj na przechwytywanie ekranu  Zezwól/Zablokuj na korzystanie ze schowka  Zezwól/Zablokuj utworzenie kopii zapasowej moich danych  Zezwól/Zablokuj widoczne hasła  Zezwól/Zablokuj na debugowanie USB  Zezwól/Zablokuj na reset fabryczny  Zezwól/Zablokuj na aktualizację OTA  Agent ochrony konsoli – oprogramowanie antywirusowe:  Program antywirusowy powinien mieć obsługę w języku polskim. Platforma powinna obsługiwać systemy operacyjne:  Android: 7.x, 7.x (KNOX), 8.x, 8.x (KNOX), 9.x, 9.x (KNOX), 10.x  10.x (KNOX), 11.x, 11.x (KNOX), 12.x, 12.x (KNOX), 13.x, 13.x (KNOX)  iOS: 12.x, 13.x, 14.x, 15.x, 16.x, 17.x |
| **Licencja** | Do 30.06.2026r |
| **Zakres prac wdrożeniowych** | Przedmiotem wdrożenia jest instalacja, konfiguracja i uruchomienie systemu ochrony stacji roboczych, laptopów i serwerów, zawierającego moduły:   1. ochrony antywirusowej oraz antymalware; 2. zaawansowanego wykrywania zagrożeń na punktach końcowych (Endpoint Detection and Response – EDR); 3. zarządzania urządzeniami końcowymi oraz zdalnego monitoringu i administracji (Remote Monitoring and Management – RMM).   Wykonawca zobowiązany jest do wykonania następujących czynności:   1. Instalacja i konfiguracja rozwiązania 2. Instalacja centralnej konsoli zarządzającej w środowisku Zamawiającego (w modelu lokalnym lub chmurowym, zgodnie z preferencją Zamawiającego). 3. Instalacja agenta bezpieczeństwa oraz agenta zarządzającego na wskazanych urządzeniach końcowych. 4. Konfiguracja polityk bezpieczeństwa, w tym:  * wykrywania zagrożeń w czasie rzeczywistym; * ochrony przed złośliwym oprogramowaniem; * kontroli aplikacji; * zapobiegania utracie danych (DLP); * reagowania na incydenty (EDR); * harmonogramu automatycznych skanów.  1. Konfiguracja monitorowania stanu technicznego urządzeń (RMM), w tym:  * zdalnej diagnostyki; * aktualizacji oprogramowania; * alarmów i powiadomień o nieprawidłowościach; * zarządzania zasobami (m.in. dyski, RAM, CPU, sieć); * zdalnego wsparcia technicznego (zdalny pulpit, przesyłanie plików itp.).  1. Testy poprawności działania 2. Przeprowadzenie testów funkcjonalnych i bezpieczeństwa. 3. Symulacja detekcji zagrożeń i zdalnych działań naprawczych. 4. Walidacja logów i powiadomień w systemie zarządzania. |
| **Szkolenie** | Szkolenie dla 5 administratorów wskazanych przez Zamawiającego w zakresie:   1. obsługa konsoli centralnej; 2. analiza zdarzeń i zagrożeń; 3. konfiguracja polityk bezpieczeństwa; 4. zarządzanie urządzeniami końcowymi; 5. reagowanie na incydenty bezpieczeństwa.   Zamawiający wymaga przeprowadzenia szkolenia w formie stacjonarnej, w siedzibie Zamawiającego. Wymaga ilość godzin przewidzianych na szkolenie to 3h. |
| **Dokumentacja** | Wykonawca po zakończeniu prac wdrożeniowych musi dostarczyć dokumentację zawierającą:   1. Opis wdrożonego środowiska (schematy, komponenty, konfiguracje). 2. Rejestr urządzeń objętych ochroną. 3. Raport końcowy z wdrożenia.   Zamawiający wymaga, aby każda osoba wykonująca czynności w ramach realizacji przedmiotu zamówienia, która uzyskają dostęp do informacji niejawnych lub wrażliwych z punktu widzenia bezpieczeństwa systemów IT Zamawiającego, podpisała stosowne oświadczenie o zachowaniu poufności, według wzoru stanowiącego załącznik do Umowy. |
| **Firewall sieciowy UTM – 1 szt.** | |
| **Architektura** | 64bit |
| **Liczba rdzeni procesora** | Min. 16 |
| **Częstotliwość nominalna procesora** | Min. 2000 MHz |
| **Wymiary** | Max. 445 x 200 x 44 mm |
| **Rozmiar pamięci** | Min. 16 GB DDR4 |
| **Rozmiar pamięci masowej** | Min. 128 MB |
| **Typ pamięci** | NAND |
| **MTBF** | Min. 200 000 godzin |
| **IPsec** | Tak |
| **Porty Ethernet** | Min. 13 (10/100/1000) |
| **Porty SFP+** | Min . 4 |
| **Szeregowy port konsoli** | RJ45 |
| **Liczba gniazd M.2** | Min. 1 |
| **Monitor temperatury procesora** | Tak |
| **Monitor temperatury PCB** | Tak |
| **Monitor napięcia** | Tak |
| **Przycisk trybu** | Tak |
| **Liczba gniazd PSU** | Min. 2 |
| **Liczba wejść AC** | Min. 2 |
| **Częstotliwość (Hz)** | 47-63 |
| **Maksymalny pobór mocy** | Max. 85 W |
| **Typ chłodzenia** | Min. 4 wentylatory |
| **Diody LED** | Tak |
| **Montaż w szafie RACK** | Tak |
| **Gwarancja** | 2 lata |
| **Zakres prac wdrożeniowych** | Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja zaawansowanego routera brzegowego UTM klasy operatorskiej, przeznaczonego do obsługi głównych punktów styku sieci LAN/WAN w infrastrukturze Zamawiającego.  Wykonawca w ramach realizacji zamówienia zobowiązany jest do wykonania poniższych czynności:   1. Instalacja urządzenia 2. Montaż urządzenia w szafie teleinformatycznej zgodnie z wymaganiami Zamawiającego. 3. Zapewnienie poprawnego podłączenia z istniejącą infrastrukturą kablową. 4. Podłączenie urządzenia do systemu zasilania i weryfikacja poprawności działania sprzętowego. 5. Konfiguracja urządzenia 6. Konfiguracja interfejsów sieciowych (w tym portów światłowodowych i miedzianych). 7. Konfiguracja routingu statycznego i/lub dynamicznego (w zależności od potrzeb Zamawiającego). 8. Konfiguracja reguł bezpieczeństwa (firewall, filtrowanie ruchu). 9. Konfiguracja mechanizmów monitorowania. 10. Wdrożenie mechanizmów zarządzania (dostęp administracyjny, logowanie zdarzeń, SNMP, syslog). 11. Przeprowadzenie testów komunikacji w środowisku produkcyjnym Zamawiającego. 12. Integracja z infrastrukturą Zamawiającego 13. Wdrożenie ustawień związanych z zarządzaniem zdalnym i dostępem opartym o określone role użytkowników.   Zamawiający wymaga, aby każda osoba wykonująca czynności w ramach realizacji przedmiotu zamówienia, która uzyskają dostęp do informacji niejawnych lub wrażliwych z punktu widzenia bezpieczeństwa systemów IT Zamawiającego, podpisała stosowne oświadczenie o zachowaniu poufności, według wzoru stanowiącego załącznik do Umowy. |
| **Szkolenie** | Szkolenie dla 5 administratorów wskazanych przez Zamawiającego w zakresie:   1. podstawowej i zaawansowanej obsługi urządzenia, 2. zarządzania konfiguracją i politykami bezpieczeństwa, 3. diagnostyki i monitorowania stanu pracy urządzenia.   Zamawiający wymaga przeprowadzenia szkolenia w formie stacjonarnej, w siedzibie Zamawiającego. Wymagana ilość godzin przewidzianych na szkolenie to 4h. |
| **Dokumentacja** | Wykonawca po zakończeniu prac wdrożeniowych musi dostarczyć dokumentację zawierającą:   1. Szczegółowy opis konfiguracji urządzenia (interfejsy, trasy, reguły bezpieczeństwa). 2. Raport z testów 3. Raport końcowy z wdrożenia. |
| **System kopii zapasowych – 1 szt.** | |
| **Wymagania funkcjonalne oprogramowania** | Oprogramowanie musi umożliwiać wykonywanie kopii zapasowych oraz przywracanie danych i konfiguracji systemu na poziomie lokalnych stacji roboczych. Wymagane funkcjonalności obejmują:  Tworzenie kopii zapasowych całych dysków lub partycji, w tym sektor po sektorze, z możliwością zapisu do jednego pliku obrazu.  Tworzenie kopii zapasowych wybranych plików i folderów z możliwością kompresji i szyfrowania danych.  Obsługa backupów przyrostowych i różnicowych, umożliwiająca optymalizację przestrzeni dyskowej i przyspieszenie procesu tworzenia kopii.  Możliwość przywrócenia całego systemu operacyjnego z poziomu nośnika ratunkowego, np. pendrive'a lub płyty startowej.  Automatyczne harmonogramowanie zadań tworzenia kopii zapasowych, z możliwością konfiguracji reguł uruchamiania (np. codziennie, tygodniowo, przy starcie systemu).  Obsługa technologii szybkiego przywracania danych (np. poprzez analizę zmian delta), pozwalająca na znaczące skrócenie czasu odtworzenia systemu.  Klonowanie dysków i partycji, w tym możliwość migracji systemu na nowy dysk z automatyczną zmianą rozmiarów partycji.  Możliwość uruchomienia kopii zapasowej jako maszyny wirtualnej w środowisku zgodnym z popularnymi narzędziami do wirtualizacji.  Obsługa różnych systemów plików, w tym co najmniej: NTFS, FAT32, exFAT, ReFS.  Kompatybilność z systemami partycjonowania MBR i GPT.  Ochrona obrazów kopii zapasowych przed nieautoryzowanym dostępem, w tym mechanizmy zabezpieczające przed modyfikacją lub usunięciem kopii przez złośliwe oprogramowanie (np. ransomware).  Interfejs użytkownika w języku angielskim lub polskim, z możliwością wyboru trybu ciemnego (dark mode) oraz dostępem do logów i raportów z wykonanych operacji. |
| **Wymagania dotyczące środowiska i kompatybilności** | Oprogramowanie musi być kompatybilne z systemami operacyjnymi rodziny Windows, w wersjach desktopowych, co najmniej od wersji Windows 10 wzwyż (w tym Windows 11).  Musi działać na komputerach klasy PC (stacjach roboczych) zarówno z procesorami 32-, jak i 64-bitowymi.  Musi umożliwiać tworzenie i przywracanie kopii zapasowych zarówno z poziomu działającego systemu, jak i środowiska uruchamianego z zewnętrznego nośnika (tzw. środowisko ratunkowe). |
| **Ogólne** | Licencja musi być przypisana do konkretnego urządzenia (stacji roboczej) i umożliwiać jej migrację na inny sprzęt w przypadku wymiany urządzenia.  Oprogramowanie musi być legalne, pochodzić z oficjalnego kanału dystrybucji i nie może być objęte ograniczeniami testowymi ani czasowymi.  Zamawiający zastrzega możliwość weryfikacji spełnienia wymagań funkcjonalnych przed odbiorem oprogramowania. |
| **Gwarancja** | 5 lat  Wsparcie musi obejmować:  Dostęp do wszystkich aktualizacji i nowych wersji oprogramowania w ramach linii produktowej.  Pomoc techniczną świadczoną drogą elektroniczną (system zgłoszeń, e-mail lub czat).  Możliwość pobrania aktualnej dokumentacji i instrukcji użytkownika. |
| **Zakres prac wdrożeniowych** | Przedmiotem zamówienia jest dostawa, instalacja oraz wdrożenie rozwiązania programowego umożliwiającego tworzenie pełnych i przyrostowych kopii zapasowych stacji roboczych w środowisku Zamawiającego. Oprogramowanie powinno umożliwiać szybkie przywracanie danych i całych systemów operacyjnych w przypadku awarii, infekcji, błędów użytkownika lub innych zdarzeń losowych.  Wykonawca w ramach realizacji zamówienia zobowiązany jest do wykonania poniższych czynności:   1. Instalacja i konfiguracja oprogramowania 2. Instalacja agenta backupu na stacjach roboczych wskazanych przez Zamawiającego. 3. Konfiguracja polityk backupu, w tym:  * typy kopii zapasowych (pełne, przyrostowe, różnicowe), * częstotliwość wykonywania backupów, * czas przechowywania, * lokalizacja kopii (magazyny lokalne i/lub sieciowe).  1. Konfiguracja harmonogramów i automatyzacji zadań. 2. Wdrożenie mechanizmów szyfrowania danych i ochrony hasłem. 3. Testy poprawności działania 4. Testowe wykonanie kopii zapasowej i jej odtworzenie. 5. Symulacja awarii i procedura przywracania całej stacji roboczej (bare-metal recovery). 6. Weryfikacja poprawności logów i powiadomień. |
| **Szkolenie** | Szkolenie dla 5 administratorów Zamawiającego w zakresie:   1. zarządzania politykami backupu, 2. procedur przywracania danych i całych systemów, 3. monitorowania stanu kopii zapasowych, 4. obsługi dzienników zdarzeń i raportów.   Zamawiający wymaga przeprowadzenia szkolenia w formie stacjonarnej, w siedzibie Zamawiającego. Wymagana ilość godzin przewidzianych na szkolenie to 4h. |
| **Dokumentacja** | Wykonawca po zakończeniu prac wdrożeniowych musi dostarczyć dokumentację zawierającą:   1. opis konfiguracji systemu, 2. harmonogramy i typy backupu, 3. procedury odzyskiwania danych, 4. lista zabezpieczonych urządzeń i ich status. |
| **Serwer NAS typu RACK wraz z dyskami – 2 szt.** | | |

|  |  |
| --- | --- |
| Procesor | 8-rdzeniowy/16-wątkowy procesor |
| Obudowa | Rack 2U o wymiarach maksymalnych 89 × 440 × 520 mm (wys. x szer. x gł.) wraz z szynami do montażu w szafie rack |
| Pamięć RAM | 32 GB UDIMM DDR5  Możliwość rozbudowy poprzez dołożenie kolejnych pamięci do min 192 GB (4 x 48GB) |
| Ilość obsługiwanych dysków | 12 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s o maksymalnej pojemności 24TB każdy |
| Gniazda m.2 | 2 gniazda M.2 2280 PCIe Gen 5 |
| Interfejsy sieciowe | Min. 2 porty 2,5 Gigabit sieci Ethernet (RJ45)  2 porty 10GbE (SFP+) z kompletem wkładek wielomodowych 10GbE SFP+ (poprzez dołożenie kompatybilnej karty sieciowej i wkładek SFP+ tego samego producenta)  2 porty 10GbE (10GBase-T)  Musi posiadać możliwość zamontowania (jako płatna opcja):  - dodatkowej karty sieciowej 25GbE SFP28,  - dodatkowej karty sieciowej FC 16GbE,  - dodatkowej karty sieciowej FC 32GbE,  - obsługa VLAN i Jumbo Frame. |
| Porty USB | Minimum 2 gniazdo typu A USB 3.2 Gen 2 10 Gb/s |
| Porty PCIe | Minimum 3 gniazda PCIe  2 x Gen 4 x4, 1 x Gen 4x8 (lub Gen 4x4) |
| Wskaźniki LED | HDD 1–12, stan, LAN, stan gniazda rozszerzenia pamięci masowej |
| Obsługa RAID | min. RAID 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity, RAID 5, 6, 10 + dysk zapasowy. |
| Funkcje RAID | Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD. |
| Szyfrowanie | 256-bitowe szyfrowanie AES folderów |
| Obsługiwane Systemy Operacyjne | min.:  Apple Mac OS 10.10 lub nowszy  Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux  IBM AIX 7, Solaris 10 lub nowszy UNIX  Microsoft Windows 7, 8, 10, 11  Microsoft Windows Server 2008 R2, 2012, 2012 R2 oraz 2016, 2019 oraz 2022 |
| Stacja monitoringu | Tak, w standardzie 8 licencji na podłączenie kamer. |
| Protokoły | CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP |
| Usługi | Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów. |
| Język GUI | Polski |
| Gwarancja producenta | 5 lat  Urządzenie musi być wyprodukowane zgodnie z normami ISO-9001 oraz ISO-14001 lub równoważnymi.  Urządzenie musi posiadać oznakowanie CE, świadczące o jego zgodności z obowiązującymi dyrektywami Unii Europejskiej.  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym gwarancją, uszkodzony dysk twardy pozostaje u Zamawiającego. |
| Waga | Maksymalnie 14 kg |
| System plików | Dyski wewnętrzne ZFS lub EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ |
| Funkcje ZFS | Liniowa deduplikacja, kompresja i kompakcja, Cache odczytu & ZIL |
| iSCSI | Obsługa MPIO, MC/S i SPC-3 Persistent Reservation |
| Liczba kont użytkowników | min. 4096 |
| Liczba grup | min. 512 |
| Liczba udziałów | min. 512 |
| Max ilość połączeń (CIFS) | 5000 |
| Zasilanie | Redundantne 350W (x2), 100–240 V |
| Wentylatory | Minimum 3 sztuki |
| UPS | Obsługa sieciowych awaryjnych zasilaczy UPS. |
| Zamontowane dyski 3.5” HDD | 4 dyski o pojemności minimum 22TB każdy, zgodnych z listą kompatybilną podaną przez producenta NAS, o parametrach nie gorszych niż:  512 MB cache,  7200 RPM,  MTBF - 1,2 mln,  średnie opóźnienie 4,17 ms,  szybkość transferu 281 MB/s,  w przypadku awarii dysk pozostaje u Zamawiającego |
| Zamontowane dyski 2.5” SSD | 4 dyski SSD 2.5” 4TB, zgodnych z listą kompatybilną podaną przez producenta NAS, o parametrach nie gorszych niż:  Odczyt sekwencyjny – 560 MB/s  Zapis sekwencyjny – 520 MB/s  TBW – minimum 2500  MTTF - 2 mln godzin  w przypadku awarii dysk pozostaje u Zamawiającego |
| Zakres prac wdrożeniowych | Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja i uruchomienie w infrastrukturze Zamawiającego urządzenia klasy NAS (Network Attached Storage).  Wykonawca w ramach realizacji zamówienia zobowiązany jest do wykonania poniższych czynności:  1. Instalacja sprzętowa  a) Montaż urządzenia w szafie RACK w lokalizacji wskazanej przez Zamawiającego.  b) Podłączenie do infrastruktury sieciowej i zasilającej.  c) Konfiguracja podstawowa interfejsów sieciowych, redundancji zasilania, zegara systemowego (NTP), alertów systemowych.  2. Konfiguracja logiczna  a) Utworzenie woluminów i udziałów sieciowych zgodnie z wymaganiami Zamawiającego.  b) Konfiguracja systemu plików zoptymalizowanego pod kątem obsługi dużych plików i backupu.  c) Utworzenie użytkowników i grup z przypisaniem uprawnień do zasobów.  3. Zabezpieczenia i monitoring  a) Konfiguracja alertów systemowych (email lub SNMP) dla podstawowych zdarzeń (awaria dysku, przegrzanie, spadek wydajności).  b) Włączenie funkcji ochrony przed nieautoryzowanym dostępem (w tym filtrowanie IP, autoblokowanie kont, logowanie zdarzeń).  c) Konfiguracja kopii zapasowej ustawień systemu urządzenia. |

|  |
| --- |
| **Serwer NAS typu TOWER wraz z dyskami – 2 szt.** |

|  |  |
| --- | --- |
| Procesor | 16-rdzeniowy/24-wątkowy procesor |
| Obudowa | Tower |
| Pamięć RAM | 64 GB UDIMM DDR4 |
| Ilość obsługiwanych dysków | min.. 8 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s o maksymalnej pojemności 24TB każdy |
| Gniazda m.2 | min. 2 gniazda M.2 2280 PCIe Gen 4 |
| Interfejsy sieciowe | min. 2 porty 2,5 Gigabit sieci Ethernet (RJ45) |
| Porty USB | Minimum 2 gniazda typu A USB 3.2 Gen 2 10 Gb/s |
| Thunderbolt | 2 porty Thunderbolt 4 |
| HDMI | 1 port HDMI rozdzielczość do 4096 x 2160 przy częstotliwości 30 Hz |
| Porty PCIe | Minimum 2 gniazda PCIe  1 x Gen 4 x4,  1 x Gen 4 x16, |
| Wskaźniki LED | HDD 1–8, stan, LAN, port USB, port m2 |
| Obsługa RAID | min. RAID 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity, RAID 5, 6, 10 + dysk zapasowy. |
| Funkcje RAID | Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD. |
| Szyfrowanie | 256-bitowe szyfrowanie AES folderów |
| Obsługiwane Systemy Operacyjne | min. :  Apple Mac OS 10.10 lub nowszy  Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux  IBM AIX 7, Solaris 10 lub nowszy UNIX  Microsoft Windows 7, 8, 10, 11  Microsoft Windows Server 2008 R2, 2012, 2012 R2 oraz 2016, 2019 oraz 2022 |
| Stacja monitoringu | Tak, w standardzie 8 licencji na podłączenie kamer. |
| Protokoły | CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP |
| Usługi | Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów. |
| Język GUI | Polski |
| Gwarancja producenta | 3 lata  Urządzenie musi być wyprodukowane zgodnie z normami ISO-9001 oraz ISO-14001 lub równoważnymi.  Urządzenie musi posiadać oznakowanie CE, świadczące o jego zgodności z obowiązującymi dyrektywami Unii Europejskiej.  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym gwarancją, uszkodzony dysk twardy pozostaje u Zamawiającego. |
| Waga | Maksymalnie 10 kg |
| System plików | Dyski wewnętrzne ZFS lub EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ |
| Funkcje ZFS | Liniowa deduplikacja, kompresja i kompakcja, Cache odczytu & ZIL |
| iSCSI | Obsługa MPIO, MC/S i SPC-3 Persistent Reservation |
| Liczba kont użytkowników | min. 4096 |
| Liczba grup | min. 512 |
| Liczba udziałów | min. 512 |
| Max ilość połączeń (CIFS) | 3500 |
| Zasilanie | 350W (x2), 100–240 V |
| Zamontowane dyski 3.5” HDD | 4 dyski o pojemności minimum 22TB każdy, zgodnych z listą kompatybilną podaną przez producenta NAS, o parametrach nie gorszych niż:  512 MB cache,  7200 RPM,  MTBF - 1,2 mln,  średnie opóźnienie 4,17 ms,  szybkość transferu 281 MB/s,  w przypadku awarii dysk pozostaje u Zamawiającego |
| Zamontowane dyski 2.5” SSD | 4 dyski SSD 2.5” 4TB, zgodne z listą kompatybilną podaną przez producenta NAS, o parametrach nie gorszych niż:  Odczyt sekwencyjny – 560 MB/s  Zapis sekwencyjny – 520 MB/s  TBW – minimum 2500  MTTF - 2 mln godzin  w przypadku awarii dysk pozostaje u Zamawiającego |
| Zakres prac wdrożeniowych | Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja i uruchomienie w infrastrukturze Zamawiającego urządzenia klasy NAS (Network Attached Storage).  Wykonawca w ramach realizacji zamówienia zobowiązany jest do wykonania poniższych czynności:  1. Instalacja sprzętowa  a) Montaż urządzenia w szafie RACK w lokalizacji wskazanej przez Zamawiającego.  b) Podłączenie do infrastruktury sieciowej i zasilającej.  c) Konfiguracja podstawowa interfejsów sieciowych, redundancji zasilania, zegara systemowego (NTP), alertów systemowych.  2. Konfiguracja logiczna  a) Utworzenie woluminów i udziałów sieciowych zgodnie z wymaganiami Zamawiającego.  b) Konfiguracja systemu plików zoptymalizowanego pod kątem obsługi dużych plików i backupu.  c) Utworzenie użytkowników i grup z przypisaniem uprawnień do zasobów.  3. Zabezpieczenia i monitoring  a) Konfiguracja alertów systemowych (email lub SNMP) dla podstawowych zdarzeń (awaria dysku, przegrzanie, spadek wydajności).  b) Włączenie funkcji ochrony przed nieautoryzowanym dostępem (w tym filtrowanie IP, autoblokowanie kont, logowanie zdarzeń).  c) Konfiguracja kopii zapasowej ustawień systemu urządzenia. |

|  |  |
| --- | --- |
| **Dyski do NAS – 6 szt.** | |
| **Dysk twardy** | Serwery NAS |
| **Pojemność** | min. 22 TB |
| **Obudowa** | 3,5” |
| **Interfejs** | SATA 6Gb/s |
| **Pamięć podręczna** | min. 512 MB |
| **Prędkość obrotowa** | min. 7200 (obr./min.) |
| **Obciążenia** | min. 180 TB/rok |
| **Przeciętne opóźnienie** | min. 4,17 ms |
| **Czujniki** | min. czujnik wstrząsów, czujnik drgań |
| **Zaawansowane technologie** | min. NCQ, AF |
| **MTBF** | min. 1,2 mln godzin rocznie |
| **Niskie zużycie energii** | max. 7 W (aktywnie) |
| **Gwarancja** | 5 lat  W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. |