SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

## Zakup i dostawa sprzętu IT wraz z oprogramowaniem w ramach projektu grantowego Cyfrowa Gmina

## 1. DOSTAWA, MONTAŻ I URUCHOMIENIE Serwera wraz z oprogramowaniem

| L. P | Komponent | Minimalne wymagania |
|---|---|---|
| | **Obudowa** | Obudowa typu Tower z możliwością instalacji do 8 dysków twardych 3,5”.<br>Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| | **Płyta główna** | Z możliwością instalacji dwóch fizycznych procesorów, posiadająca minimum 16 slotów na pamięć RAM RDIMM z możliwością zainstalowania do minimum 1TB pamięci RAM, możliwe zabezpieczenia pamięci: ECC. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym. |
| | **Procesor** | Zainstalowane dwa procesory min. 8-rdzeniowe klasy x86, min. 2.8GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 130 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| | **Pamięć RAM** | 128 GB pamięci RAM RDIMM o częstotliwości taktowania minimum 3200MHz |
| | **Sloty PCI Express** | Funkcjonujące sloty PCI Express:<br>- minimum 3 sloty PCI Express Gen4 |
| | **Interfejsy sieciowe/FC/SAS** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT |
| | **Dyski twarde** | Możliwość instalacji dysków twardych 3,5” typu: SATA, NearLine SAS, SAS, SSD.<br>Zainstalowane:<br>5 dysków SAS o pojemności min. 600GB, Hot-Plug<br>Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |

| | | |
|---|---|---|
| | | Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony 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. |
| | **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących. |
| | **Wbudowane porty** | Minimum 5 portów USB z czego min. 2 w technologii 3.0<br>1x VGA<br>Możliwość rozbudowy o port RS-232 |
| | **Video** | Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1920x1200 pikseli |
| | **Zasilanie** | redundantne zasilacze o mocy minimum 800W wraz z kablami zasilającymi. |
| | **Diagnostyka i Bezpieczeństwo** | zintegrowany z płytą główną moduł TPM 2.0 |
| | **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego, karta zarządzająca, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:<br>zdalny dostęp do graficznego interfejsu Web karty zarządzającej;<br>wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;<br>możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera oraz z możliwością rozszerzenia funkcjonalności o:<br>zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);<br>szyfrowane SSL<br>wsparcie dla IPv6;<br>możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;<br>integracja z Active Directory;<br>wsparcie dla dynamic DNS;<br>wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.<br>możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera<br>możliwość obsługi przez sześciu użytkowników jednocześnie;<br>możliwość podmontowania zdalnych wirtualnych napędów;<br>wirtualną konsolę z dostępem do myszy, klawiatury;<br>możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; |
| | **Oprogramowanie do zarządzania** | Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: |

| | | |
|---|---|---|
| | | Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych<br>integracja z Active Directory<br>Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta<br>Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish<br>Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram<br>Szczegółowy opis wykrytych systemów oraz ich komponentów<br>Możliwość eksportu raportu do CSV, HTML, XLS, PDF<br>Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.<br>Grupowanie urządzeń w oparciu o kryteria użytkownika<br>Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji<br>Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach<br>Szybki podgląd stanu środowiska<br>Podsumowanie stanu dla każdego urządzenia<br>Szczegółowy status urządzenia/elementu/komponentu<br>Generowanie alertów przy zmianie stanu urządzenia.<br>Filtry raportów umożliwiające podgląd najważniejszych zdarzeń<br>Integracja z service desk producenta dostarczonej platformy sprzętowej<br>Możliwość przejęcia zdalnego pulpitu<br>Możliwość podmontowania wirtualnego napędu<br>Kreator umożliwiający dostosowanie akcji dla wybranych alertów<br>Możliwość importu plików MIB<br>Przesyłanie alertów „as-is” do innych konsol firm trzecich<br>Możliwość definiowania ról administratorów<br>Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów<br>Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)<br>Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta<br>Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów<br>Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. |

| | | |
|---|---|---|
| | | Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.<br>Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile<br>Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.<br>Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.<br>Zdalne uruchamianie diagnostyki serwera.<br>Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.<br>Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| | **Warunki gwarancji** | 3 lata gwarancji producenta<br>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.<br>Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.<br>Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.<br>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.<br>Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.<br>Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.<br>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.<br>Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.<br>Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. |

| | | |
|---|---|---|
| | | Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.<br>Możliwość rozszerzenia gwarancji przez producenta do 7 lat.<br>Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.<br>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. |
| | **System Operacyjny – w formularzu należy podać pełną nazwę oprogramowania.** | Serwerowy system operacyjny Microsoft Windows Serwer 2022 – wraz z 35 licencjami CAL dla użytkowania<br>lub równoważny:<br>kryteria równoważności : Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości.<br>Wbudowane wsparcie instalacji i pracy na wolumenach które:<br>- pozwalają na zmianę rozmiaru w czasie pracy systemu,<br>- umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,<br>- umożliwiają kompresję „w locie" dla wybranych plików i/lub folderów,<br>- umożliwiają zdefiniowanie list kontroli dostępu (ACL).<br>Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.<br>Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.<br>Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.<br>Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.<br>Wbudowana zapora internetowa (firewall) z obsługi definiowanych reguł dla ochrony połączeń internetowych i intranetowych.<br>Graficzny interfejs użytkownika.<br>Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.<br>Możliwość zmiany języka interfejsu po zainstalowaniu systemu dla co najmniej języka polskiego i angielskiego.<br>Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. |

| | | |
|---|---|---|
| | | Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.<br>Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).<br>Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:<br>- podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,<br>- usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarzadzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:<br>• podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,<br>• ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,<br>• odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.<br>Zdalna dystrybucja oprogramowania na stacje robocze.<br>Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.<br>PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:<br>• dystrybucję certyfikatów poprzez http,<br>• konsolidację CA dla wielu lasów domeny,<br>• automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.<br>Szyfrowanie plików i folderów.<br>Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).<br>Serwis udostępniania stron WWW.<br>Wsparcie dla protokołu IP w wersji 6 (Ipv6).<br>Wbudowane usługi VPN pozwalające na zestawienie równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows. |
| | **Oprogramowanie zabezpieczające serwer – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania** | System chroniący przed zagrożeniami, posiadający certyfikaty: OPSWAT Platinum, AV-Test 'Top Product', AV Comperative Advance +, ISO 27001 . Silnik musi umożliwiać co najmniej:<br>• wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,<br>• wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,<br>• stosowanie kwarantanny,<br>• wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) |

| | | |
|---|---|---|
| | | • skanowanie urządzeń USB natychmiast po podłączeniu,<br>• automatyczne odłączanie zainfekowanej końcówki od sieci,<br>• skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji.<br>• Zarządzanie „aktywami" stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach.<br>• Musi posiadać moduł ochrony IDS/IPS<br>• Musi posiadać mechanizm wykrywania skanowania portów<br>• Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów<br>• Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości<br>Szyfrowanie danych:<br>• Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.<br>• Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.<br><br>Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.<br>Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.<br>Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.<br>Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.<br>Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware.<br>Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.<br>Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. |

| | | |
|---|---|---|
| | | Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.<br>Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware<br>Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:<br>• Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli<br>• Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory<br>• Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux<br>• Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.<br>• Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich<br>• Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji<br>Zarządzanie przez Chmurę:<br>1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach<br>2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury<br>3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur<br>4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy<br>5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach<br>6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń<br>7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej<br><br>Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.<br>Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania. |

| | | |
|---|---|---|
| | | 1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer<br>2. Oprogramowanie klienckie, zarządzane z poziomu serwera.<br>System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:<br>• różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie<br>• funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD<br>• funkcje regulowania połączeń WiFi i Bluetooth<br>• funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe<br>• funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi<br>• funkcje blokowania dostępu dowolnemu urządzeniu<br>• możliwość tymczasowego dodania dostępu do urządzenia przez administratora<br>• zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu<br>• możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka<br>• możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora<br>• możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry<br>• możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich<br>• funkcję wirtualnej klawiatury<br>• możliwość blokowania każdej aplikacji<br>• możliwość zablokowania aplikacji w oparciu o kategorie<br>• możliwość dodania własnych aplikacji do listy zablokowanych<br>• zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze<br>• dodawanie innych aplikacji<br>• dodawanie aplikacji w formie portable<br>• możliwość wyboru pojedynczej aplikacji w konkretnej wersji<br>• dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB<br>• kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool<br>• możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.<br>• możliwość zablokowania funkcji Printscreen<br>• funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx<br>• funkcje monitorowania i kontroli przepływu poufnych informacji |

| | | |
|---|---|---|
| | | • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików<br>• możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj<br>• możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe<br>• ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe<br>• ochrona zawartości schowka systemu<br>• ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL<br>• możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych<br>• ochrona plików zamkniętych w archiwach<br>• Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem<br>• możliwość tworzenia profilu DLP dla każdej polityki<br>• wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania<br>• ochrona przez wyciekiem plików poprzez programy typu p2p<br>Monitorowanie zmian w plikach:<br>• Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.<br>• Funkcje monitorowania określonych rodzajów plików.<br>• Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.<br>• Generator raportów do funkcjonalności monitora zmian w plikach.<br>• możliwość śledzenia zmian we wszystkich plikach<br>• możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach<br>• możliwość definiowana własnych typów plików<br>Optymalizacja systemu operacyjnego stacji klienckich:<br>• usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku<br>• optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem<br>• możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich<br>• instruktaż stanowiskowy pracowników Zamawiającego<br>• dokumentacja techniczna w języku polskim<br>Wspierane platformy i systemy operacyjne:<br>1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)<br>2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)<br>3. Mac OS X, Mac OS 10<br>4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat<br><br>Platforma do zarządzania dla Android i iOS:<br>• Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę |

| | | |
|---|---|---|
| | | • Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.<br>Zarządzanie użytkownikiem<br>• Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email<br>• Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika<br>• Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi<br>• Musi posiadać możliwość eksportu danych użytkownika<br>Zarządzanie urządzeniem<br>• Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO<br>• Musi umożliwiać import listy urządzeń z pliku CSV<br>• Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych<br>• Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta<br>• Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał<br>• Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres<br>• Musi zawierać podgląd aktualnie zainstalowanych aplikacji<br>• Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych,<br>• Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł<br>• Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres<br><br>Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:<br>Wymagania dotyczące technologii:<br>1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową<br>2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.<br>3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:<br>- Microsoft Internet Explorer<br>- Microsoft Edge<br>- Mozilla Firefox<br>- Google Chrome |

| | | |
|---|---|---|
| | | - Safari<br>4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących<br>5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie<br>6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:<br>- Windows 2008 R2<br>- Windows 2012<br>- Windows 2012 R2<br>- Windows 2016<br>7. Portal zarządzający musi umożliwiać:<br>a) przegląd wybranych danych na podstawie konfigurowalnych widgetów<br>b) zablokowania możliwości zmiany konfiguracji widgetów<br>c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.<br>d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności<br>e) eksport wszystkich skanów podatności do pliku CSV |
| | **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001<br>Serwer musi posiadać deklaracja CE.<br>Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.**<br>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022. |

| | | |
|---|---|---|
| | **System bazodanowy** | 1. Musi mieć możliwość wykorzystania jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Musi zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL.<br>2. Musi mieć zintegrowane narzędzia graficzne do zarządzania systemem – musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania.<br>3. Musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.<br>4. Musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.<br>5. Musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).<br>6. Musi umożliwiać tworzenie klastrów niezawodnościowych.<br>7. Musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech:<br>a. bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam serwer relacyjnej bazy)<br>b. niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe)<br>c. klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach<br>8. Musi pozwalać na kompresję kopii zapasowej danych (backup) w trakcie jej tworzenia. Musi to być cecha niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.<br>9. Musi mieć możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania musi wspierać następujące algorytmy szyfrujące: AES 128, AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych.<br>10. Musi mieć możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową.<br>11. Musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność. |

| | | |
|---|---|---|
| | | 12. Musi posiadać możliwość rejestracji zdarzeń na poziomie silnika relacyjnej bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń.<br>13. Wymagana jest rejestracja zdarzeń:<br>a. odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system)<br>b. wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur)<br>c. para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy)<br>14. Musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci.<br>15. Musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniuje się typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków" obiektu, „rodzica" itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez dostawcę języka programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji.<br>16. Musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:<br>a. udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli<br>b. udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD<br>c. udostępniać język zapytań do struktur XML<br>d. udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML)<br>e. udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań<br>17. Musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności:<br>a. zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów<br>b. oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp. |

| | | |
|---|---|---|
| | | c. obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań serwera relacyjnej bazy danych<br>d. typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja (punkt), seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.)<br>18. Musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań. Musi umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo musi udostępniać środowisko do debuggowania.<br>19. Musi udostępniać wbudowany mechanizm umożlwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny.<br>20. Musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.<br>21. Musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.<br>22. Musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze w konywane przez silnik bazy danych w ten sam sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji SBD, wprowadzeniu zmian sprzętowych serwera.<br>23. Musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.:<br>a. mechanizm debuggowania tworzonego rozwiązania<br>b. mechanizm stawiania „pułapek” (breakpoints)<br>c. mechanizm logowania do pliku wykonywanych przez transformację operacji<br>d. możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu)<br>e. możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo)<br>f. mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli) |

| | | |
|---|---|---|
| | | g. mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach)<br>h. mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego<br>i. mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiany źródła danych<br>24. Musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (kostki OLAP).<br>25. Musi być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji.<br>26. Musi być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar bLokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina."<br>27. Musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów.<br>28. Musi mieć możliwość składowania w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań.<br>29. Musi być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail).<br>30. Musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki).<br>31. Musi posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych.<br>32. Musi obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).<br>33. Musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych.<br>34. Musi pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu.<br>35. Musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez system protokołem http (dostęp klienta za pomocą przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania musi obsługiwać:<br>a. raporty parametryzowane<br>b. cache raportów (generacja raportów bez dostępu do źródła danych) |

| | | |
|---|---|---|
| | | c. cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów)<br>d. współdzielenie predefiniowanych zapytań do źródeł danych<br>e. wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File)<br>f. możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport<br>g. możliwość wizualizacji wskaźników KPI<br>h. możliwość wizualizacji danych w postaci obiektów sparkline<br>36. Musi mieć możliwość osadzania i administrowania z wykorzystaniem mechanizmu Web Serwisów (Web Services). Wymagane jest generowanie raportów min. w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF. Dodatkowo raporty powinny być eksportowane w formacie Atom data feeds, które można będzie wykorzystać jako źródło danych w innych aplikacjach.<br>37. Musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów.<br>38. Musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja).<br>39. Musi posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.<br>40. Musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache'u przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD.<br>41. Musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań.<br>42. Musi udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit). |

## 2. DOSTAWA Komputerów stacjonarnych typu All-In-One – 10 sztuk

| **Szczegółowy opis** | | |
|---|---|---|
| Komputer stacjonarny typu All In One.<br><br>W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy (numer konfiguracji lub part numer) oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.<br>Jeśli na stronie internetowej producenta nie jest dostępna pełna oferta modeli sprzętu wraz z jego konfiguracją, do oferty należy dołączyć katalog producenta zaoferowanego produktu umożliwiający weryfikację oferty pod kątem zgodności z wymaganiami Zamawiającego.<br><br>Nie dopuszcza się zaoferowania komputera odnawianego. | | |
| Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SIWZ. W tym celu Wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 5 dni od daty otrzymania wezwania, próbkę oferowanego sprzętu. W odniesieniu do programowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana przez Komisję Przetargową na zasadzie spełnia / nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki (oferty) z treścią SIWZ. | | |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
| 1. | **Procesor** | Procesor klasy x86, zaprojektowany do wydajnej pracy w komputerach stacjonarnych.<br>Procesor musi osiągać w testach SYSMark 25 minimum 1625 punktów.<br>Wyniki testu należy załączyć do oferty.<br>Testy muszą zostać przeprowadzone na konfiguracji zaoferowanej zamawiającemu:<br>• zachowanie modelu procesora<br>• zachowanie taktowania, ilości i pojemności pamięci RAM<br>• zachowanie modelu dysku SSD<br>• zachowanie modelu płyty głównej<br>zachowanie rodziny systemu operacyjnego |
| 2. | **Pamięć operacyjna RAM** | Min. 16 GB 4800MHz non-ECC |

| | | |
|---|---|---|
| 3. | **Parametry pamięci masowej** | M.2 500 GB SSD PCIe 3.0 NVMe<br>Możliwość montażu dodatkowego dysku 2,5” SSD lub HDD |
| 4. | **Karta graficzna** | Karta graficzna zintegrowana w procesorze komputera.<br>Karta musi osiągać w teście SYSMark 25 Creativity minimum 1750 punków |
| 5. | **Wyposażenie multimedialne** | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.<br>Wbudowane w obudowie komputera: głośniki stereo (2x3W)<br>Port słuchawek i mikrofonu (dopuszcza się złącze typu COMBO)<br>Kamera video z mechaniczną zasłoną obiektywu o rozdzielczości min. 5 MPix i wsparciem dla Windows Hello<br>Dwa mikrofony wbudowane w obudowę komputera |
| 6. | **Obudowa** | - Zintegrowana z monitorem (AIO)<br>- Obudowa trwale oznaczona nazwą producenta, nazwą komputera, part numberem, numerem seryjnym<br>- Możliwość podpięcia linki zabezpieczającej przez zintegrowane z obudową złącze np. Kensington Lock, Noble Lock |
| 7. | **Płyta główna** | Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej. |
| 8. | **Zgodność z systemami operacyjnymi** | Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera ). |
| 9. | **Bezpieczeństwo** | TPM 2.0 |
| 10. | **Wirtualizacja** | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji). |

| | | |
|---|---|---|
| 11. | **BIOS** | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera.<br><br>Pełna obsługa BIOS za pomocą klawiatury i myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:<br><br>- wersji BIOS wraz z datą produkcji BIOS<br>- nr seryjnym komputera<br>- Ilości zainstalowanej pamięci RAM<br>- typie procesora i jego prędkości<br>- MAC adresu zintegrowanej karty sieciowej<br>- nr seryjnym płyty głównej komputera<br>- informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS<br><br>Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:<br><br>- Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS<br>- Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej.<br>- Funkcja bezpiecznego usuwania danych z dysku |
| 12. | **Ekran** | Matowy, matryca IPS lub WVA, 23,8” z podświetleniem w technologii LED<br><br>Rozdzielczość FHD 1920x1080,<br><br>Jasność min. 250nits, kontrast 1000:1 |

| | | |
|---|---|---|
| | | Podstawa komputera umożliwiająca regulację wysokości (do 100mm) i pochylenia |
| 13. | **Interfejsy / Komunikacja** | Wyposażony w minimum:<br>3x USB typ C w tym min. 2 USB w standardzie 3.x<br>3x USB typ A w tym min. 2 USB w standardzie 3.x<br>1x RJ-45<br>1x HDMI out w standardzie min. 2.0<br>1x HDMI in w standardzie min. 1.4<br>1x port słuchawek i mikrofonu (dopuszcza się złącze typu COMBO) |
| 14. | **Karta sieciowa LAN** | RJ-45 - 100/1000 |
| 15. | **Karta sieciowa WLAN** | Wbudowana karta sieciowa, pracująca w standardzie AX 2x2<br>Bluetooth 5.1 |
| 16. | **Klawiatura i mysz** | Klawiatura bezprzewodowa w układzie US.<br>Mysz bezprzewodowa z rolką (scroll)<br>Klawiatura i mysz działające na jednym adapterze lub za pomocą połączenia bluetooth. |
| 17. | **Zasilacz** | Energooszczędny zasilacz o sprawności min. 85 % i mocy nie mniejszej niż 150W |
| 18. | **Certyfikaty, oświadczenia i standardy** | ENERGY STAR min. 8.0<br>EPEAT na poziomie min. Silver<br>Deklaracja zgodności CE<br>Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki<br>Certyfikat ISO 9001 dla producenta komputera |

| | | |
|---|---|---|
| | | Certyfikat ISO 14001 dla producenta komputera<br><br>Certyfikat ISO 50001 dla producenta komputera |
| 19. | **Waga/Wymiary** | Waga urządzenia z podstawą nie może przekraczać 8 kg. |
| 20. | **System operacyjny** | Microsoft Windows 11 Pro 64 bit lub system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:<br><br>1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:<br><br>a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,<br><br>b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych<br><br>2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego<br><br>3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim<br><br>4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.<br><br>5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe<br><br>6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,<br><br>7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.<br><br>8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim<br><br>9. Wbudowany system pomocy w języku polskim.<br><br>10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). |

| | | |
|---|---|---|
| | | 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.<br><br>12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.<br><br>13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.<br><br>14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.<br><br>15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.<br><br>16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".<br><br>17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.<br><br>18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.<br><br>19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.<br><br>20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.<br><br>21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.<br><br>22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.<br><br>23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."<br><br>24. Wbudowany mechanizm wirtualizacji typu hypervisor." |

| | | |
|---|---|---|
| | | 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.<br><br>26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.<br><br>27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.<br><br>28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).<br><br>29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.<br><br>30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.<br><br>31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.<br><br>32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM<br><br>33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.<br><br>34. Możliwość tworzenia wirtualnych kart inteligentnych.<br><br>35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)<br><br>36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.<br><br>37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.<br><br>38. Mechanizmy logowania w oparciu o: |

| | | |
|---|---|---|
| | | a. Login i hasło,<br>b. Karty inteligentne i certyfikaty (smartcard),<br>c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),<br>d. Certyfikat/Klucz i PIN<br>e. Certyfikat/Klucz i uwierzytelnienie biometryczne<br>39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5<br>40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.<br>41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach<br>42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń<br>43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń |
| 21. | **Oprogramowanie do aktualizacji sterowników** | Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. |
| 22. | **Gwarancja** | Minimalny czas trwania gwarancji producenta wynosi 3 lata, świadczona w miejscu użytkowania sprzętu (on-site).<br>Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.<br>W przypadku niewywiązywania się z obowiązku serwisowego przez Autoryzowanego Partnera Serwisowego lub Wykonawcę producent przejmie na siebie obowiązek serwisowy.<br>Komputery musza pochodzić z polskiej dystrybucji producenta. |

| | | |
|---|---|---|
| | | Zamawiający może wystąpić do wykonawców o oświadczenie producenta komputera, potwierdzające spełnienie ww. warunków. |
| 23. | **Wsparcie techniczne producenta** | ▪ Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera<br>▪ Bezpośredni kontakt z Autoryzowanym Partnerem Serwisowym Producenta (brak konieczności zgłaszania każdej usterki sprzętowej telefonicznie), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki.<br>▪ Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera<br>▪ Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-18:00<br>Wsparcie techniczne świadczone przez producenta lub autoryzowanego partnera serwisowego dla urządzeń i preinstalowanego oprogramowania OEM, zakupionego z urządzeniem, dostarczane zdalnie.<br><br>Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta.<br><br>Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta. |
| 24. | **Procedura testowania** | Testy SYSmark® 25 muszą być wykonane w konfiguracji komputera identycznej z wymaganą przy rozdzielczości ekranu 1920x1080 pixeli/60 Hz, 32-bitowej głębi koloru.<br>Wymaga się przeprowadzenia testów SYSmark® 25 na systemie operacyjnym w wersji zgodnej z oferowaną (Home, Professional lub Edu), ale nie starszym wydaniem niż 21H2.<br>Testy muszą zostać wykonane z włączonymi wszystkimi ustawieniami z zakładki „Required” oraz „Recommended”. Nie dopuszcza się używania w teście żadnej opcji z zakładki „Optional”.<br>Nie dopuszcza się modyfikacji ustawień BIOS (w tym overclockingu) w celu osiągnięcia wyższej wydajności urządzenia.<br>W przypadku użycia przez Wykonawcę testu BAPCo do oceny wydajności Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych testów Wykonawca musi dostarczyć Zamawiającemu oprogramowanie testujące wraz z licencją, zestaw komputerowy w konfiguracji identycznej z wymaganą oraz |

| | | |
|---|---|---|
| | | dokładne opisy użytych testów wraz z wynikami w formacie PDF w terminie nie dłuższym niż 7 dni od otrzymania zawiadomienia od Zamawiającego. |

## 3. Firewall UTM – z licencją na rok

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań

| **Parametr** | **Wymagania minimalne** |
|---|---|
| **Wymagania Ogólne** | System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.<br>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.<br>System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.<br>System wspiera protokoły IPv4 oraz IPv6 w zakresie:<br>Firewall.<br>Ochrony w warstwie aplikacji.<br>Protokołów routingu dynamicznego. |
| **Redundancja, monitoring i wykrywanie awarii** | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.<br>Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. |

| Parametr | Wymagania minimalne |
|---|---|
| | Monitoring stanu realizowanych połączeń VPN.<br>System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |
| **Interfejsy, Dysk, Zasilanie** | System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:<br>10 portami Gigabit Ethernet RJ-45.<br>System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.<br>System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.<br>System jest wyposażony w zasilanie AC. |
| **Parametry wydajnościowe** | W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.<br>Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.<br>Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.<br>Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.<br>Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.<br>Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.<br>Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps. |
| **Funkcje Systemu Bezpieczeństwa** | W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:<br>1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.<br>2. Kontrola Aplikacji.<br>3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.<br>4. Ochrona przed malware.<br>5. Ochrona przed atakami - Intrusion Prevention System.<br>6. Kontrola stron WWW.<br>7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.<br>8. Zarządzanie pasmem (QoS, Traffic shaping).<br>9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).<br>10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.<br>11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. |

| Parametr | Wymagania minimalne |
|---|---|
| | 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.<br>13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |
| **Polityki, Firewall** | 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.<br>2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:<br>• Translację jeden do jeden oraz jeden do wielu.<br>• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.<br>3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.<br>4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.<br>5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.<br>6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.<br>7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.<br>• Amazon Web Services (AWS).<br>• Microsoft Azure.<br>• Cisco ACI.<br>• Google Cloud Platform (GCP).<br>• OpenStack.<br>• VMware NSX.<br>• Kubernetes. |
| **Połączenia VPN** | 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:<br>• Wsparcie dla IKE v1 oraz v2.<br>• Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).<br>• Obsługa protokołu Diffie-Hellman grup 19, 20.<br>• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.<br>• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.<br>• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.<br>• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.<br>• Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. |

| Parametr | Wymagania minimalne |
|---|---|
| | • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.<br>• Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.<br>• Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.<br>• Mechanizm „Split tunneling" dla połączeń Client-to-Site.<br>2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:<br>• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.<br>• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.<br>• Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |
| **Routing i obsługa łączy WAN** | W zakresie routingu rozwiązanie zapewnia obsługę:<br>Routingu statycznego.<br>Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).<br>Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.<br>Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.<br>ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.<br>BFD (Bidirectional Forwarding Detection).<br>Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |
| **Funkcje SD-WAN** | System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.<br>SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| **Zarządzanie pasmem** | System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.<br>SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| **Ochrona przed malware** | Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).<br>Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. |

| Parametr | Wymagania minimalne |
|---|---|
| | System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.<br>System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.<br>System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).<br>Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.<br>System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.<br>Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.<br>Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| **Ochrona przed atakami** | Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.<br>System chroni przed atakami na aplikacje pracujące na niestandardowych portach.<br>Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.<br>System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.<br>System dysponuje sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.<br>Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).<br>Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.<br>Wykrywanie i blokowanie komunikacji C&C do sieci botnet.<br>Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| **Kontrola aplikacji** | Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.<br>Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. |

| Parametr | Wymagania minimalne |
|---|---|
| | Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.<br>Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.<br>Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).<br>System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |
| **Kontrola WWW** | Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.<br>W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.<br>Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.<br>Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.<br>Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).<br>Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.<br>Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.<br>Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.<br>System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| **Uwierzytelnianie użytkowników w ramach sesji** | System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:<br>Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.<br>Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.<br>Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.<br>System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.<br>System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.<br>Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| **Zarządzanie** | Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.<br>Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. |

| Parametr | Wymagania minimalne |
|---|---|
| | Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.<br>System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.<br>System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.<br>Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.<br>Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.<br>Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).<br>Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| **Logowanie** | Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.<br>W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.<br>Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.<br>Możliwość włączenia logowania per reguła w polityce firewall.<br>System zapewnia możliwość logowania do serwera SYSLOG.<br>Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| **Certyfikaty** | Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:<br>ICSA lub EAL4 dla funkcji Firewall. |
| **Testy wydajnościowe oraz funkcjonalne** | Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy. |
| **Serwisy i licencje** | Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:<br>Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Sygnatury ochrony systemów przemysłowych SCADA na okres 12 miesięcy. |
| **Gwarancja oraz wsparcie** | Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |

| Parametr | Wymagania minimalne |
|---|---|
| **Rozszerzone wsparcie serwisowe AHB/SOS** | System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy.<br>System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:<br>Wsparcie telefoniczne zespołu certyfikowanych inżynierów.<br>Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.<br>Doradztwo w zakresie konfiguracji.<br>Zdalne wsparcie techniczne.<br>Pomoc w zakładaniu zgłoszeń serwisowych u producenta.<br>Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).<br>Przygotowanie urządzenia do zdalnej konfiguracji.<br>Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.<br>Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.<br>Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.<br>Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.<br>Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.<br>Wymagania powinny być potwierdzone dokumentami:<br>Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).<br>Certyfikat ISO 9001 podmiotu serwisującego.<br>Szkolenie on-line w zakresie obsługi zakupionego sprzętu i oprogramowania. |