ZAŁĄCZNIK NR 1B DO SWZ

Znak sprawy: Rzp.271.1.4.2025

**Formularz Parametrów Technicznych – Część 2**

**Oprogramowanie EDR plus serwer**

|  |
| --- |
| **System EDR – do 75 stanowisk**  |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje****Wykonawca** **Wymogi dotyczące opisu oferowanych parametrów:**TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcęNIE – wykonawca nie spełnia konkretnego parametru |
| **Ochrona stacji roboczych - Windows** |
| **1.** | * Rozwiązanie musi wspierać systemy operacyjne Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11.
* Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
* Rozwiązanie musi wspierać architekturę ARM64.
* Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
* Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
* Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim.
* Skuteczność rozwiązania potwierdzona nagrodami VB100 i AV-comparatives.
 | TAK |  |
| **Ochrona antywirusowa i antyspyware** |
| **1.** | * Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
* Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
* Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
* Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje.
* Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
* Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
* Rozwiązanie musi posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
* Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
* Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
* Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
* Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych.
* Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
* Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
* Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
* Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
* Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
* Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
* W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
* Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
* Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
* Rozwiązanie musi posiadać wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
* Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
* Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
* Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
* Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
* Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
* Rozwiązanie musi posiadać możliwość blokowania możliwości przeglądania wybranych stron internetowych. Rozwiązanie musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
* Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
* Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
* Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
* Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
* Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
* Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego.
* Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
* Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
* Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
* W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
* Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
* Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
* Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
* Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
* Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
* Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
* Rozwiązanie musi posiadać możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji rozwiązanie musi pytać o hasło.
* Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo.
* Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
* Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
* Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
* System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
* System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
* Rozwiązanie musi posiadać umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
* Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
* Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
* Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
* Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
* W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
* Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
* Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS).
* Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,• tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,• tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.* Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
* Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
* Rozwiązanie musi posiadać zaawansowany skaner pamięci.
* Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
* Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
* Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
* Rozwiązanie musi posiadać posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
* Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
* Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
* Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji.
* Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
* Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
* Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
* Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
* Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
* W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania.
* Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
* Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
* Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
* Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.
* Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie.
* W trakcie instalacji rozwiązanie ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM.
* W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
* Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej.
* Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
* Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
* Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
* Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.
* Rozwiązanie musi posiadać możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
* Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
* Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
* Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
* Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
* Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
* Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
* Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.
* Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
* Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
* Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
* Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
* Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet.
* Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB.
* Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
* Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
 | TAK |  |
| **Ochrona przed spamem** |
| **1.** | * Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
* Rozwiązanie musi umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
* Rozwiązanie musi umożliwiać automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
* Rozwiązanie musi posiadać możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
* Rozwiązanie musi posiadać możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
* Rozwiązanie musi posiadać możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
* Rozwiązanie musi możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
* Rozwiązanie musi domyślnie współpracować z folderem „Wiadomości-śmieci”, dostępnym w programie Microsoft Outlook.
* Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana”
* Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana”.
* Rozwiązanie musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.
 | TAK |  |
| **Zapora osobista (personal firewall)** |
| **1.** | * Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
* tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
* tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
* tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
* tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
* Rozwiązanie musi oceniać reguły zapory systemu Windows.
* Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych.
* Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
* Rozwiązanie musi posiadać możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.
* Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
* Rozwiązanie musi posiadać możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
* Rozwiązanie musi posiadać możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
* Rozwiązanie musi wykrywać modyfikację w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.
* Rozwiązanie musi posiadać możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
* Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
* Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
* Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
* Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
* Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
* Rozwiązanie musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów:
* z aplikacją lokalną, którą administrator wskazuje z listy,
* z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.
 | TAK |  |
| **Kontrola dostępu do stron internetowych** |
| **1.** | * Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
* Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory.
* Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
* Podstawowe kategorie, w jakie rozwiązanie musi być wyposażone to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
* Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych.
* Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta.
* Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
* Rozwiązanie musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj.
* Rozwiązanie musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej.
 | TAK |  |
| **Bezpieczna przeglądarka** |
| **1.** | * Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
* Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
* Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki.
* Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę.
* Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki.
* Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
 | TAK |  |
| **Ochrona serwera Windows** |
| **1.** | * Rozwiązanie musi posiadać wsparcie dla systemów Microsoft Windows Server 2008 R2 i nowszych.
* Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
* Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
* Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
* Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
* Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje.
* Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
* Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
* Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
* Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
* Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
* Rozwiązanie ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
* Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych.
* Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
* Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
* Rozwiązanie musi wspierać mechanizm klastrowania.
* Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS).
* Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
* tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
* tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
* tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
* tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
* tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
* Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
* Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
* Rozwiązanie musi posiadać zaawansowany skaner pamięci.
* Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
* Rozwiązanie musi oferować możliwość skanowania dysków sieciowych typu NAS.
* Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze.
* Rozwiązanie musi umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
* Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
* Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
* Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
* Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
* Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
* W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
* Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
* Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
* Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
* Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
* Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
* Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
* Rozwiązanie ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
* Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
* Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
* Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
* Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
* Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
* Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
* W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
* Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
* Rozwiązanie musi posiadać możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
* Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo.
* Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i wyświetlić listę niezainstalowanych aktualizacji.
* Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje
* krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
* Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
* System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
* System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
* Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
* Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
* Rozwiązanie musi oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
* Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
* Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
* Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
* Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
* Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
* Rozwiązanie musi być wyposażone w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
* Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
* Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
* Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
* Rozwiązanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania.
* Rozwiązanie musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”.
* Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
* Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.
* Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
* Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
* Rozwiązanie musi posiadać ochronę przed przyłączeniem komputera do sieci botnet.
* Rozwiązanie musi mieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
* Rozwiązanie musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów.
* Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
* Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
* Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
* Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
 | TAK |  |
| **Administracja zdalna** |
| **1.** | * Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019 oraz systemach Linux.
* Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.
* Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
* Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.
* Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
* Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
* Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
* Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy.
* Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.
* Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.
* Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.
* Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
* Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym.
* Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
* Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
* Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
* Serwer administracyjny musi posiadać wsparcie dla „VDI” oraz „Golden Master Image”.
* Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów.
* Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy.
* Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
* Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
* Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS.
* Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP.
* Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11.
* Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap.
* Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych.
* Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów.
* Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
* Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
* Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.
* Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS.
* Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
* Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
* Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
* Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania.
* Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
* Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.
* W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play.
* Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
* Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS.
* Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
* Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.
* Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
* Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
* Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
* Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.
* Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.
* Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
* Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
* Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.
* Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
* Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
* Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
* Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
* Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
* Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.
* Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
* Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.
* Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.
* Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
* Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.
* Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta.
* Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
* Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
* Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
* Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.
* Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
* Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.
* Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może
* zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF lub CSV.
* Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
* Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.
* Powiadomienia mailowe mają być wysyłane w formacie HTML.
* Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.
* Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
* Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
* Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
* Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.
* Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.
* W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
* Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
* Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.
* Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
* Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.
* W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.
* Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.
* Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.
* Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.
* Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.
* Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.
* Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych.
* 9Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault).
* Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk.
* Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal).
* Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.
 | TAK |  |
| **Sandbox w chmurze**  |
| **1.** | * Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
* Rozwiązanie musi wykorzystywać do działania chmurę producenta.
* Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
* Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
* Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
* Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
* Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
* Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
* Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
* Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
* Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
* Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
* Czysty,
* Podejrzany,
* Bardzo podejrzany,
* Szkodliwy.
* W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
* 1W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
 | TAK |  |
| **Endpoint Detection and Response**  |
|  | **Serwer*** Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych.
* Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
* System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.
* Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
* Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
* Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
* Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
* Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
* Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
* Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
* Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
* Serwer musi posiadać ponad 800 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
* Serwer administracyjny musi posiadać możliwość uruchomienia reguł w oparciu o dane historyczne.
* Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
* Serwer musi posiadać możliwość ustawiania priorytetu zdarzeń z użyciem 4-stopniowej skali.
* Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
* Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
* Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
* W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
* W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
* Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie wprowadzonej nazwy.
* Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
* Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal).
* Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
* Konsola administracyjna musi mieć możliwość tagowania obiektów.
* Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli.
* Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci.
* Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
* Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł.

**Agent*** Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10 oraz Windows Server 2008/2012/2016/2019.
* Pełne wsparcie dla systemów macOS 10.12 i nowszych.
* Wsparcie dla 32 i 64-bitowej wersji systemu Windows.
* Agent musi współpracować z produktem antywirusowym tego samego producenta.
* Agent nie może działać bez produktu antywirusowego tego samego producenta.
* W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonanej przez agenta.
* Połączenie agenta do serwera zarządzającego musi być szyfrowane.
* Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane.
 |  |  |

**Serwer**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje****Wykonawca** **Wymogi dotyczące opisu oferowanych parametrów:**TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcęNIE – wykonawca |
| 1 | Obudowa Rack o wysokości max 2U z możliwością instalacji do 10 dysków 3.5” lub z możliwością instalacji do 16 dysków 2,5’’ Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |  |  |
| 2 | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |  |
| 3 | Chipset Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |  |  |
| 4 | Zainstalowane jeden procesor ośmiordzeniowy klasy x86, dedykowane do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. **80** w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. |  |  |
| 5 | RAM - 128GB RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 32 sloty przeznaczonych do instalacji pamięci.Płyta główna powinna obsługiwać do minimum 768Gb pamięci RAM. |  |  |
| 6 | Zabezpieczenia pamięci RAM - Memory Rank Sparing, Memory Mirror |  |  |
| 7 | Interfejsy sieciowe/FC/SAS. Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseTDodatkowo zainstalowane karty:* karta minimum dwuportowa 10Gb SFP+. Karty dostarczyć wraz z wkładkami 10GBASE-LR lub SR. Patchcordy odpowiedniego typu o wymaganej długości. Zastosowanie do połączenia serwera z przełącznikiem w szafie.
* jedna karta FC 16Gb
 |  |  |
| 8 | Dyski twarde. Możliwość instalacji dysków SATA, SAS, SSD.Zainstalowane dyski:6 dysków 4TB 7,2k RPM NLSAS 3,5“ lub SSD - skonfigurowane w RAID 6 lub 8 dysków 2,4T 10k RPM SAS skonfigurowane w RAID 6 |  |  |
| 9 | Kontroler RAID. Sprzętowy kontroler dyskowy, posiadający min. 4GB nieulotnej pamięci cache, wymagane konfiguracje poziomów RAID: 1, 5, 6. |  |  |
| 10 | Wbudowane porty* min. 1 port USB 2.0 oraz 2 porty USB 3.0,
* minimum 1 port video
 |  |  |
| 11 | VideoZintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1440x900 |  |  |
| 12 | WentylatoryRedundantne |  |  |
| 13 | ZasilaczeRedundantne, Hot-Plug o mocy co najmniej 700W każdy z dedykowanymi przewodami zasilającymi. Wykonawca powinien dopasować moc zasilaczy do zaproponowanej konfiguracji serwera. |  |  |
| 14 | BezpieczeństwoPłyta wyposażona w moduł TPM. |  |  |
| 15 | DiagnostykaDiody umieszczone na froncie obudowy. |  |  |
| 16 | Karta ZarządzaniaNiezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
* zdalne monitorowanie i informowanie o statusie serwera
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
* możliwość podmontowania zdalnych wirtualnych napędów;
* wirtualną konsolę z dostępem do myszy, klawiatury;
* wsparcie dla Ipv6;
* SNMP; IPMI2.0, SSH,
* integracja z Active Directory;
* możliwość obsługi przez dwóch administratorów jednocześnie;
* wysyłanie do administratora maila z powiadomieniem o awarii
 |  |  |
| 17 | Certyfikaty* Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001
* Serwer musi posiadać deklaracja CE
 |  |  |

**NAS Klasy Enterprise – 2 szt.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje****Wykonawca** **Wymogi dotyczące opisu oferowanych parametrów:**TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcęNIE – wykonawca |
|  | Architektura procesora 64-bitowy x86 |  |  |
|  | Procesor min. 4-rdzeniowy/4-wątkowy procesor o taktowaniu bazowym 2.0 GHz , zwiększanym do 2,9 GHz |  |  |
|  | Koprocesor arytmetyczny FPU |  |  |
|  | Mechanizm szyfrowania (AES-NI) |  |  |
|  | Transkodowanie wspomagane sprzętowo |  |  |
|  | Pamięć systemowa min. 8 GB RAM |  |  |
|  | Pamięć flash min. 4 GB (ochrona systemu operacyjnego przed podwójnym rozruchem) |  |  |
|  | Wnęka dysków min. 12 dyski 3,5-calowe SATA 6 Gb/s, 3 Gb/s |  |  |
|  | Kompatybilność dysków 3,5-calowe zatoki:3,5-calowe dyski twarde SATA2,5-calowe dyski SSD SATA |  |  |
|  | Wymieniany podczas pracy |  |  |
|  | Gniazdo M.2 poprzez kartę PCIe |  |  |
|  | Obsługa przyspieszenia pamięci podręcznej SSD |  |  |
|  | Port 2,5 Gigabit Ethernet (2,5G/1G/100M) min. 2 porty |  |  |
|  | Port 10 Gigabit sieci Ethernet Zainstalowana karta 2x 10GB sfp+ , należy dostarczyć 4 wkładki sfp+ SR , oraz niezbędne okablowanie |  |  |
|  | Wake on LAN (WOL) |  |  |
|  | Ramka Jumbo |  |  |
|  | Port USB 2.0 min. 2  |  |  |
|  | Port USB 3.2 Gen 2 (10 Gb/s) min. 2 |  |  |
|  | Montaż maks. 2U |  |  |
|  | liczba połączeń współbieżnych (CIFS) — z maks. pojemnością pamięci min. 1500  |  |  |
|  | Wielkość puli min. 308 TB |  |  |
|  | Ilość storage-puli min. 128 |  |  |
|  | Typy wolumenów Thick, Thin, Static |  |  |
|  | Wielkość wolumenu min. 250 TB |  |  |
|  | JBOD Expansio |  |  |
|  | VJBOD / VJBOD Cloud |  |  |
|  | iSCSI Service |  |  |
|  | Fibre Channel Service |  |  |
|  | LUN Type Thick, Thin |  |  |
|  | File-based iSCSI LUN |  |  |
|  | Block-based iSCSI LUN |  |  |
|  | Wielkość LUN min. 250 TB |  |  |
|  | Ilość targetów LUN min. 128 |  |  |
|  | Funkcjonalności LUN:1. LUN Mapping (LUN can be moved between iSCSI and FC)2. LUN Masking3. WWPN Aliases Import/Export4. FC Port Group5. FC Port Binding6. Multipath IO (MPIO)7. Online LUN capacity expansion8. LUN snapshot9. LUN snapshot replication and clone |  |  |
|  | Auto Tiering |  |  |
|  | Dyski Twarde SSD 4 szt. , Oferowane dyski twarde musza znajdować się na liście kompatybilności producenta oferowanego NAS.

|  |  |
| --- | --- |
| Typ dysku | SSD  |
| Format szerokości | 2,5'' (SFF)  |
| Typ napędu | Wewnętrzny  |
| Pojemność dysku min. | 1.92 TB  |
| Interfejs dysku | SATA III - 6 Gb/s  |
| TBW | 3504 TB  |
| Prędkość odczytu min. | 560 MB/s  |
| Prędkość zapisu min. | 530 MB/s  |
| Ilość operacji odczytu IOPS (min.) | 94 K  |
| Ilość operacji zapisu IOPS (min.) | 78 K  |

 |  |  |
|  | Dyski Twarde Talerzowe 6 szt., Oferowane dyski twarde musza znajdować się na liście kompatybilności producenta oferowanego NAS.

|  |  |
| --- | --- |
| Typ dysku | HDD  |
| Format szerokości | 3,5'' (LFF)  |
| Typ napędu | Wewnętrzny  |
| Pojemność dysku min. | 12 TB  |
| Interfejs dysku | SATA III - 6 Gb/s  |
| Prędkość obrotowa min. | 7200 obr/min  |
| Bufor min. | 256 MB  |
| Wielkość sektora dysku | 4Kn  |
| Ilość operacji odczytu IOPS (min.) | 170 K  |
| Ilość operacji zapisu IOPS (min.) | 550 K  |
| Czas pracy pomiędzy awariami (MTBF) | 2500000 h  |
| Nieprzerwana praca 24/7 | Tak  |
| Pobór mocy maks. | 8.6 W  |
| Pobór mocy maks. (czuwanie) | 4.4 W  |
|  |

 |  |  |

1. Przełącznik LAN – 3 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje****Wykonawca** **Wymogi dotyczące opisu oferowanych parametrów:**TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcęNIE – wykonawca |
| Lp. | Parametry |  |  |
| 1 | Charakterystyka sprzętowa |  |  |
| 48 x 1000Base-T IEEE 802.3ab |  |  |
| Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). |  |  |
| Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. |  |  |
| 4 x SFP+ IEEE 802.3ae/802.3ae;- porty SFP+ muszą obsługiwać również moduły SFP 1000Base-X IEEE 802.3z; Dostarczenie taką ilość kabli stackowych i taką ilość wkładek sfp+, aby wykonać konfigurację stack na tych trzech przełącznikach i obsadzić pozostałe porty wkładkami sfp+ |  |  |
| Konsola szeregowa RS-232. |  |  |
| Łączenie urządzeń w stosy o wielkości co najmniej 6 jednostek. Awaria żadnego pojedynczego urządzenia nie może spowodować przerwania pracy stosu. Praca w topologii pierścienia. Przepustowość magistrali stosu co najmniej 40 Gb/s. Port-Channel oraz Mirroring ruchu przy użyciu dowolnych portów w stosie. |  |  |
| Zasilanie AC 230V. |  |  |
| Pojemność przełączania nie mniej, niż 176 Gb/s. Wydajność przełączania nie mniej niż 130 Mp/s. |  |  |
| Architektura nieblokującą (wire-speed). |  |  |
| Pojemność tablicy MAC nie mniej, niż 16K. Możliwość wprowadzenia co najmniej 510 wpisów statycznych. |  |  |
| Ilość RAM nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 32 MB. |  |  |
| Obsługa ramek Jumbo o rozmiarze co najmniej 9210 B. |  |  |
| Bufor pakietów nie mniej, niż 3 MB. |  |  |
| Temperatura pracy w zakresie co najmniej od -5C do 50 stopni Celsjusza. |  |  |
| MTBF > 410000 godzin. |  |  |
| Obudowa urządzenia powinna być wyposażona w mocowanie umożliwiające przypięcie zabezpieczenia fizycznego typu Kensington Lock. |  |  |
| 2 | Funkcjonalności warstwy 2 |  |  |
| IGMP Snoopingv3- obsługa nie mniej, niż 510 grup multicast w tym co najmniej 256 grup statycznych. |  |  |
| MLD Snoopingv2- obsługa nie mniej, niż 31 grup multicast w tym co najmniej 31 grup statycznych. |  |  |
| IEEE 802.1D, 802.1w, 802.1s (co najmniej 16 instancji). Funkcja 802.1Q Restricted Role oraz 802.1Q Restricted TCN. |  |  |
| Wykrywanie pętli w L2 dla przyłączonych urządzeń bez protokołu rodziny STP. |  |  |
| Tworzenie interfejsów Port-Channel - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie z obsługą LACP. |  |  |
| LLDP (802.1AB) oraz LLDP-MED. |  |  |
| ERPS (ITU-T G.8032) w wersji co najmniej 1. Jednoczesna obsługa co najmniej 1 pierścieni. |  |  |
| DHCP Relay w tym opcji 60 i 61 oraz opcji 82, DHCP Local Relay + opcja 82. DHCP Relay dla IPv6. |  |  |
| Port monitoring/mirroring/span. Możliwość monitorowania tylko wybranego ruchu. |  |  |
| Obsługa sieci VLAN |  |  |
| 802.1Q VLAN, co najmniej 4094, 802.1v GVRP. |  |  |
| Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. |  |  |
| Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN. |  |  |
| Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN. |  |  |
| 3 | Funkcjonalności warstwy 3 |  |  |
| Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 16 takich interfejsów. |  |  |
| Przełącznik musi posiadać funkcjonalność Gratuitous ARP. |  |  |
| Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na wskazany adres IP w sieci. |  |  |
| Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 10 pule adresów IP oraz wspierającego protokół IPv6 przydzielającego minimum 16 pule adresów IP. |  |  |
| Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 0,5K wpisów oraz umożliwiać wprowadzenie co najmniej 256 wpisów statycznych. |  |  |
| Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 510 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 256 takich tras dla IPv6. |  |  |
| Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 60 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 32 takich tras dla IPv6. |  |  |
| Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 60 takich tras) oraz dla IPv6 (co najmniej 30 tras). |  |  |
| Urządzenie musi być wyposażone w funkcję Floating Static Route (tworzenie zapasowych domyślnych/statycznych tras routingu dla danej podsieci docelowej) dla IPv4. |  |  |
| Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery. |  |  |
| 4 | Quality of Service |  |  |
| Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6. |  |  |
| Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR. |  |  |
| Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. |  |  |
| Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. |  |  |
| 5 | Filtrowanie ruchu |  |  |
| Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza. |  |  |
| Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN. |  |  |
| 6 | Funkcje bezpieczeństwa |  |  |
| Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 120 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. |  |  |
| Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. |  |  |
| Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. |  |  |
| Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. |  |  |
| Urządzenie musi wspierać funkcję umożliwiającą zmianę przypisanych z serwera RADIUS uprawnień bez rozłączania ponownego uwierzytelniania przyłączonego klienta. |  |  |
| Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. |  |  |
| Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN. |  |  |
| Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania. |  |  |
| Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 250 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. |  |  |
| Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). |  |  |
| Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP. |  |  |
| Przełącznik powinien mieć możliwość definiowania globalnie dla urządzenia adresów MAC, z/do których ruch nie będzie obsługiwany. |  |  |
| Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci. |  |  |
| Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU. |  |  |
| Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service. |  |  |
| Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Multicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Broadcast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie. |  |  |
| Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast. |  |  |
| 7 | Zarządzanie |  |  |
| Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. |  |  |
| Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP. |  |  |
| Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. |  |  |
| Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. |  |  |
| W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. |  |  |
| Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych urządzeń. |  |  |
| Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. |  |  |
| Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON i obsługiwać protokół sFlow. |  |  |
| Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. |  |  |
| Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. |  |  |
| Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. |  |  |
| Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6. |  |  |
| Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6. |  |  |
| Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci. |  |  |
| Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego. |  |  |
| Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6, a także umożliwiać przeglądanie tablicy adresów MAC. |  |  |
| Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia. |  |  |
| Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia. |  |  |
| Urządzenie powinno być w stanie wysyłać powiadomienia SNMP (tzw. SNMP Traps) w przypadku pojawienia się w sieci nowego adresu MAC. |  |  |
| Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane. |  |  |
| Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware. |  |  |
| Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików. |  |  |
| Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet). |  |  |
| Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych. |  |  |
| 8 | Pozostałe |  |  |
| Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania. |  |  |
|  |

**System do backup, serwer, biblioteka taśmowa**

**System do backup**

Wymagania dla oprogramowania:

1. W celu zapewnienia dużej elastyczności i skalowalności środowiska kopii zapasowych oprogramowanie systemu powinno posiadać trójwarstwową architekturę: Serwer Zarządzający, Serwer Mediów, Klient.

2. Oprogramowanie systemu powinno umożliwiać wykonywanie kopii zapasowych w środowisku heterogenicznym za pomocą, dedykowanego dla platformy systemowej, klienta systemu kopii zapasowych.

3. System powinien umożliwiać łatwą rozbudowę w miarę rozrastania się infrastruktury informatycznej Zamawiającego, poprzez dokładanie kolejnych centralnie zarządzanych Serwerów Mediów.

4. Proponowane rozwiązanie musi umożliwiać uruchomienie serwera zarządzającego kopiami zapasowymi na głównych platformach Windows i Linux.

5. Proponowane rozwiązanie musi wspierać wysoką dostępność (klastrowanie) serwera kontrolującego kopie zapasowe.

6. Oprogramowanie musi być niezależne pod względem sprzętowym i nie może preferować instalacji na platformie sprzętowej jednego producenta. Powinno udostępniać te same funkcjonalności niezależnie od tego na jakiej platformie systemowej będzie zainstalowane. Zamawiający musi posiadać możliwość zmiany platformy sprzętowej bez utraty funkcjonalności systemu kopii zapasowej.

7. Proponowane rozwiązanie musi wspierać wdrożenia na sprzęcie fizycznym, infrastrukturze wirtualnej, w chmurze oraz w kontenerach

8. Proponowane rozwiązanie musi umożliwiać administrację za pomocą GUI (aplikacja lub web),

9. System powinien posiadać centralną konsolę zarządzania środowiskiem kopii zapasowych. Konsola musi umożliwiać:

9.1 monitorowanie i zarządzanie wszystkimi zadaniami wykonywania i odtwarzania kopii zapasowych, tworzenia duplikatów wykonanych kopii zapasowych,

9.2 ustawianie harmonogramów wykonywania kopii zapasowych,

9.3 monitorowanie i kontrolowanie urządzeń składowania kopii zapasowych podłączonych do Serwerów Mediów,

9.4 centralne zarządzanie konfiguracją, właściwych dla oprogramowania systemu, ustawień Serwera Zarządzającego, Serwera Mediów, Klientów,

9.5 uruchomienie odtwarzania kopii zapasowych na klienta systemu

10. Oprogramowanie systemu musi posiadać obsługę z poziomu wiersza poleceń w systemach Linux, Unix i Windows. Obsługa z poziomu wiersza poleceń musi umożliwiać:

10.1 konfigurację i modyfikację polityk wykonywania kopii zapasowych,

10.2 konfigurację i modyfikację harmonogramów wykonywania kopii zapasowych,

10.3 konfigurację i modyfikację urządzeń składowania kopii zapasowych podłączonych do Serwerów Mediów,

10.4 konfigurację i modyfikację nośników taśmowych,

10.5 monitorowanie i kontrolowanie zadań kopii zapasowych,

10.6 konfigurację i modyfikację nośników taśmowych

10.7 konfigurację i modyfikację właściwych dla oprogramowania systemu, ustawień Serwera Zarządzającego, Serwera Mediów, Klientów,

10.8 konfigurację, modyfikację i przeglądanie dzienników Serwera Zarządzającego, Serwera Mediów, Klientów,

11. Rozwiązanie powinno być dostępne także jako zintegrowane programowo i sprzętowo urządzenie (appliance), a więc sprzęt i oprogramowanie backupowe razem. Zintegrowane urządzenia powinny umożliwiać zbudowanie w pełni funkcjonującej trzywarstwowej architektury backupowej z funkcjonalnością deduplikacji danych.

12. Baza katalogowa dla systemu backupowego musi być częścią systemu backupowego i wspierać platformy minimum Linux oraz Windows oraz nie powinna posiadać ograniczeń wynikających z ilości używanych w serwerze procesorów i rdzeni procesorów.

13. Baza katalogowa musi być w cenie systemu kopii zapasowych i nie ograniczona co do ilości środowisk backupowych, mocy czy ilości serwerów czy to backupowych czy produkcyjnych. Jakakolwiek rozbudowa środowiska backupowego czy dodanie następnego nie może powodować konieczności dokupienia licencji dla tej bazy.

14. Oprogramowanie systemu kopii zapasowych musi posiadać zintegrowane zarządzanie kluczami szyfrującymi oraz musi posiadać możliwość integracji z zewnętrznymi usługami zarządzania kluczami szyfrowania,

15. Oprogramowanie systemu kopii zapasowych musi integrować się z urządzeniami dyskowymi (deduplikatory) wspierającymi mechanizm WORM w celu ochrony danych przed zaszyfrowaniem, modyfikacją i usunięciem. Funkcjonalność musi zapewniać, że obraz kopii zapasowej jest tylko do odczytu i nie może być modyfikowany, uszkodzony lub zaszyfrowany po utworzeniu kopii zapasowej oraz chronić obraz kopii zapasowej przed usunięciem przed upływem terminu ważności.

17. Proponowane rozwiązanie musi wspierać ochronę klientów pracujących pod kontrolą:

17.1 Windows 7 - 11

17.2 Windows Server 2008 - 2022, w tym wydania półroczne

17.3 Oracle Linux 6.8 i nowsze

17.4 Oracle Solaris 10 Update 11 i nowsze na architekturach Sparc i x64

18. Proponowane rozwiązanie musi wspierać architekturę składowania kopii zapasowych D2D2T i D2D2C.

19. Proponowane rozwiązanie musi obsługiwać dowolny typ pamięci dyskowej (DAS, NAS, SAN) dla repozytorium backupu.

20. Proponowane rozwiązanie musi wspierać storage taśmowy (samodzielne napędy taśmowe oraz biblioteki taśmowe w tym m.in. biblioteki robotów sterowane ACS) głównych producentów.

21. Proponowane rozwiązanie musi deduplikować dane na źródle i celu.

22. Deduplikacja musi umożliwiać wybór pomiędzy zmiennym i stałym rozmiarem bloku. Rozmiar bloku musi umożliwiać jego wybór.

23. Proponowane rozwiązanie musi wspierać deduplikację zarówno inline jak i postprocesową

24. Proponowane rozwiązanie musi wspierać urządzenia deduplikacyjne głównych producentów takich jak Dell EMC, Exagrid, HPE, Quantum, NEC

25. Proponowane rozwiązanie musi obsługiwać wirtualne biblioteki taśmowe (VTL)

26. Proponowane rozwiązanie musi wspierać transfer danych zarówno przez sieć LAN jak i SAN

27. Proponowane rozwiązanie musi wspierać głównych dostawców chmur publicznych jako magazyn kopii zapasowych

28. Proponowane rozwiązanie musi obsługiwać deduplikację do chmury w celu minimalizacji transferu danych

29. Proponowane rozwiązanie musi umożliwiać wznowienie nieudanego zadania backupowego od ostatniego punktu kontrolnego

30. Proponowane rozwiązanie musi automatyzować tworzenie wielu kopii zapasowych na różnych urządzeniach magazynowych z różną długością przechowywania danych.

31. Proponowane rozwiązanie powinno posiadać możliwość wykonywania wysokowydajnych kopii zapasowych serwerów z bardzo obciążonymi systemami plików na dyskach z dużą liczbą plików (np. backup typu disk-image)

32. Proponowane rozwiązanie musi zapewniać możliwość wykonywania backupu syntetycznego

33. Proponowane rozwiązanie musi umożliwiać tworzenie ręcznych kopii zapasowych ad-hoc

34. Proponowane rozwiązanie musi wspierać topologie replikacji danych typu jeden-do-jednego, wiele-do-jednego, jeden-do-wielu oraz kaskadową z wykorzystaniem deduplikacji danych w celu zminimalizowania ilości przesyłanych danych

35. Proponowane rozwiązanie musi wspierać szyfrowanie danych

36. Proponowane rozwiązanie musi umożliwiać wznowienie nieudanego zadania przywracania z ostatniego punktu kontrolnego

37. Proponowane rozwiązanie musi zapewniać funkcje umożliwiające natywne odzyskiwanie "bare metal" (w pełni zautomatyzowane odzyskiwanie obejmujące system operacyjny, konfigurację, aplikacje i dane) klientów Windows, Linux, Solaris bez konieczności korzystania z zewnętrznych/rodzimych narzędzi do odzyskiwania/reimaging systemu operacyjnego.

38. Proponowane rozwiązanie musi umożliwiać przywracanie różnych konfiguracji systemu oraz różnych układów dysków.

39. Proponowane rozwiązanie musi zapewniać możliwość konwersji P2V i V2P

40. Proponowane rozwiązanie musi umożliwiać przywracanie nawet po wygaśnięciu wsparcia technicznego oprogramowania

41. Proponowane rozwiązanie musi umożliwiać przywracanie pojedynczych obiektów Active Directory z kopii zapasowej Windows System State

Backup oprogramowania do wirtualizacji fizycznych maszyn

1. Proponowane rozwiązanie musi wspierać Microsoft Hyper-V 6.2 i nowsze użytkowane przez Zamawiającego

3. Proponowane rozwiązanie musi wspierać ochronę maszyn wirtualnych rezydujących na systemach plików NTFS, ReFS, Windows Storage Spaces, Storage Spaces Direct oraz SMB 3.0

4. Proponowane rozwiązanie musi wspierać Resilient Change Tracking (RCT)

5. Proponowane rozwiązanie musi wspierać tworzenie syntetycznych kopii zapasowych (tworzonych na podstawie ostatniego pełnego i przyrostowego backupu RCT) maszyn wirtualnych w celu umożliwienie tworzenia kopii zapasowych przyrostowych na zawsze

6. Proponowane rozwiązanie musi wspierać ograniczenie liczby aktywnych snapshotów lub backupów na serwer i klaster

7. Proponowane rozwiązanie musi zawierać mechanizm automatycznego wykrywania i ochrony maszyn wirtualnych bez konieczności zmiany polityk backupu.

8. Proponowane rozwiązanie musi umożliwiać wykluczenie usuniętych bloków i plików swap z kopii zapasowej maszyny wirtualnej

9. Proponowane rozwiązanie musi wspierać wyłączenie dysków startowych z backupu maszyn wirtualnych Hyper-V z kopii zapasowych maszyn wirtualnych

10. Proponowane rozwiązanie musi wspierać wyłączenie dysków danych z backupu maszyn wirtualnych kopii zapasowej maszyny wirtualnej

11. Proponowane rozwiązanie musi wspierać przywracanie pojedynczego pliku z kopii zapasowej maszyny wirtualnej Hyper-V bez konieczności przenoszenie dysku wirtualnego w lokalizacji tymczasowej, jeżeli obraz kopii zapasowej jest przechowywany na taśmach

12. Proponowane rozwiązanie musi zapewniać integrację z System Center Virtual Machine Manager (SCVMM) w celu umożliwienia odzyskiwania maszyn wirtualnych

Backup MS SQL Server

1. Proponowane rozwiązanie musi wspierać Microsoft SQL Server 2014 i nowsze

2. Proponowane rozwiązanie musi wspierać SQL Server Availability Groups

3. Proponowane rozwiązanie musi wspierać automatyczne wykrywanie instancji SQL

4. Proponowane rozwiązanie nie powinno wymagać skryptów wsadowych tworzonych przez użytkownika, które posiadały instrukcje tworzenia kopii zapasowych instancji baz danych SQL oraz logów transakcyjnych

5. Proponowane rozwiązanie musi zapewniać wykonywanie pełnych, różnicowych i dzienników transakcji kopii zapasowych baz danych SQL

6. Proponowane rozwiązanie nie może wykorzystywać metody log-shipping do ochrony logów transakcyjnych SQL

7. Proponowane rozwiązanie musi umożliwiać wykonywanie kopii zapasowych MS SQL Server poza hostem SQL Server, Instant Recovery oraz wykonywanie kopii zapasowych u dostawcy sprzętu.

8. Proponowane rozwiązanie musi wspierać pełne przywracanie i odzyskiwanie baz danych SQL

9. Proponowane rozwiązanie musi wspierać przywracanie grup plików SQL

10. Proponowane rozwiązanie musi wspierać przywracanie plików bazy danych SQL

11. Proponowane rozwiązanie musi wspierać przywracanie logów transakcyjnych SQL do określonego punktu w czasie

12. Proponowane rozwiązanie musi wspierać przywracanie logu transakcyjnego SQL do określonego punktu w czasie konkretnej transakcji

Backup NDMP

1. Proponowane rozwiązanie musi wspierać wykorzystanie protokołu Network Data NDMP (Network Data Management Protocol) do inicjowania i sterowania kopiami zapasowymi i przywracaniem systemów NAS (Network Attached Storage)

2. Proponowane rozwiązanie musi obsługiwać NDMP v2, v3 i v4

3. Proponowane rozwiązanie musi wykorzystywać techniki wykrywania zmian w filerze w celu identyfikacji modyfikacji, które nastąpiły od momentu wykonania ostatniego backupu

4. Proponowane rozwiązanie musi obsługiwać lokalne i trójstronne kopie zapasowe NDMP

5. Proponowane rozwiązanie musi obsługiwać funkcję NDMP DirectCopy

6. Proponowane rozwiązanie musi umożliwiać przywracanie pojedynczych plików z kopii zapasowych NDMP

7. Proponowane rozwiązanie musi obsługiwać funkcję NDMP Direct Access Recovery (DAR)

Raportowanie

1. Proponowane rozwiązanie musi posiadać możliwość centralnego zarządzania, monitorowanie i raportowanie w odniesieniu do środowisk oprogramowania i urządzeń, w tym wielu środowisk backupowych

2. Proponowane rozwiązanie musi umożliwiać wysyłanie powiadomień o zadaniach za pomocą poczty elektronicznej lub SNMP

Odporność na Ransomware

1. Proponowane rozwiązanie musi posiadać wbudowany mechanizm wykrywania i powiadamiania o podejrzanych zmianach podczas tworzenia kopii zapasowych

2. Proponowane rozwiązanie musi posiadać własny skaner złośliwego oprogramowania oraz mieć możliwość integracji z zewnętrznymi skanerami złośliwego oprogramowania w celu skanowania składowanych obrazów kopii zapasowych

3. Proponowane rozwiązanie musi posiadać możliwość automatycznego wstrzymywania zadań kopii zapasowych dla chronionego zasobu po wykryciu infekcji w jego kopii zapasowej, powinno obejmować tworzenie nowych kopii zapasowych, ich powielanie i wygaszanie

4. Proponowane rozwiązanie musi posiadać możliwość identyfikowania ostatniej znanej dobrej kopii zapasowej przed przywróceniem maszyny wirtualnej

Pakiet godzin serwisowych w ilości nie mniejszej niż 20 (określona w kryterium) godzin do wykorzystania w okresie do 09.04.2026 r.

**Biblioteka taśmowa**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje****Wykonawca** **Wymogi dotyczące opisu oferowanych parametrów:**TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcęNIE – wykonawca |
| 1 | Obudowa przystosowana do montażu w standardowej szafie rack 19’’. Maksymalna wysokość oferowanego rozwiązania - 3U. |   |  |
| 2 | Biblioteka taśmowa musi być wyposażona w min. 1 napęd taśmowy LTO7 z interfejsem FC. |   |  |
| 3 | Biblioteka taśmowa musi mieć możliwość rozbudowy do min. 3 napędów taśmowych. |   |  |
| 4 | Biblioteka musi być wyposażona w nie mniej niż 35 sloty na taśmy z możliwością rozbudowy do 270 slotów, poprzez dodatkowe moduły rozszerzeń. |   |  |
| 6 | Biblioteka musi być wyposażona w przynajmniej 5 slotów wejścia/wyjścia (tzw. mail slot), umożliwiający wymianę taśm bez konieczności wyłączania urządzenia. |   |  |
| 7 | Biblioteka musi być wyposażona w czytnik kodów kreskowych. |    |  |
| 8 | Biblioteka musi być wyposażona w komplet magazynków na taśmy, tak by możliwa była pełna obsada biblioteki taśmami LTO. |   |  |
| 9 | Możliwość zdalnego zarządzania biblioteki poprzez interfejs WWW. |    |  |
| 10 | Możliwość monitorowania stanu biblioteki i napędów. |    |  |
| 11 | Biblioteka musi posiadać panel sterowania oraz wyświetlacz informujący o błędach urządzenia, aktywności napędów. |   |  |
| 12 | Biblioteka powinna umożliwiać partycjonowanie. Każda partycja powinna być prezentowana do hosta jako niezależna biblioteka. |   |  |
| 13 | Razem z biblioteką oferent powinien dostarczyć min. 10 taśm LTO7 RW oznaczonych kodami kreskowymi oraz 2 taśmy czyszczące.  |   |  |
| 14 | Do biblioteki należy dostarczyć: Niezbędne kable sygnałowe FC, do podłączenia biblioteki do serwera. |    |  |
| 15 | Niezbędne kable zasilające.  |    |  |
| 16 | Dostarczone urządzenie musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu (najnowsza wersja firmware na dzień dostawy). |   |  |
| 17 | Wszystkie oferowane urządzenia muszą być fabrycznie nowe. |    |  |
| 18 | Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. |   |  |
| 19 | Urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.  |   |  |
| 20 | Oferowane produkty (urządzenia, sprzęty) w przedmiotowym postępowaniu o udzielenie zamówienia publicznego muszą spełniać wymagania norm CE, lub równoważne. |   |  |

**Serwer**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje****Wykonawca** **Wymogi dotyczące opisu oferowanych parametrów:**TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcęNIE – wykonawca |
| 1 | Obudowa Rack o wysokości max 2U z możliwością instalacji do 10 dysków 3.5” lub z możliwością instalacji do 16 dysków 2,5’’ Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |  |  |
| 2 | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |  |
| 3 | ChipsetDedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |  |  |
| 4 | ProcesorZainstalowane jeden procesor ośmiordzeniowy klasy x86, dedykowane do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. **80** w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. |  |  |
| 5 | RAM128GB RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 32 sloty przeznaczonych do instalacji pamięci.Płyta główna powinna obsługiwać do minimum 768Gb pamięci RAM. |  |  |
| 6 | Zabezpieczenia pamięci RAMMemory Rank Sparing, Memory Mirror |  |  |
| 7 | Interfejsy sieciowe/FC/SASWbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseTDodatkowo zainstalowane karty:* karta minimum dwuportowa 10Gb SFP+. Karty dostarczyć wraz z wkładkami 10GBASE-LR lub SR. Patchcordy odpowiedniego typu o wymaganej długości. Zastosowanie do połączenia serwera z przełącznikiem w szafie.
* jedna karta FC 16Gb
 |  |  |
| 8 | Dyski twardeMożliwość instalacji dysków SATA, SAS, SSD.Zainstalowane dyski:6 dysków 4TB 7,2k RPM NLSAS 3,5“ lub SSD - skonfigurowane w RAID 6 lub8 dysków 2,4T 10k RPM SAS skonfigurowane w RAID 6 |  |  |
| 9 | Kontroler RAIDSprzętowy kontroler dyskowy, posiadający min. 4GB nieulotnej pamięci cache, wymagane konfiguracje poziomów RAID: 1, 5, 6. |  |  |
| 10 | Wbudowane porty* min. 1 port USB 2.0 oraz 2 porty USB 3.0,
* minimum 1 port video
 |  |  |
| 11 | VideoZintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1440x900 |  |  |
| 12 | WentylatoryRedundantne |  |  |
| 13 | ZasilaczeRedundantne, Hot-Plug o mocy co najmniej 700W każdy z dedykowanymi przewodami zasilającymi. Wykonawca powinien dopasować moc zasilaczy do zaproponowanej konfiguracji serwera. |  |  |
| 14 | BezpieczeństwoPłyta wyposażona w moduł TPM. |  |  |
| 15 | DiagnostykaDiody umieszczone na froncie obudowy. |  |  |
| 16 | Karta ZarządzaniaNiezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
* zdalne monitorowanie i informowanie o statusie serwera
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
* możliwość podmontowania zdalnych wirtualnych napędów;
* wirtualną konsolę z dostępem do myszy, klawiatury;
* wsparcie dla Ipv6;
* SNMP; IPMI2.0, SSH,
* integracja z Active Directory;
* możliwość obsługi przez dwóch administratorów jednocześnie;
* wysyłanie do administratora maila z powiadomieniem o awarii
 |  |  |
| 17 | Certyfikaty* Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001
* Serwer musi posiadać deklaracja CE
 |  |  |

**UPS Centralny**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje****Wykonawca** **Wymogi dotyczące opisu oferowanych parametrów:**TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcęNIE – wykonawca |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Moc wyjściowa min. 15 kVA w obszarze pracy współczynnika mocy obciążenia od 0,8 indukcyjny do 0,8 pojemności. |  |  |
|  | Ilość faz 3/3 trzy fazy wejściowe i 1 faza wyjściowa. |  |  |
|  | Wyposażony w dotykowy, graficzny wyświetlacz LCD, z komunikatami w języku polskim. |  |  |
|  | Napięcie wejściowe – wyjściowe 3x400 V zgodne z wartościami zapisanymi w Polskiej Normie PN - IEC 60038, z tolerancją minimum 325V do 475V  |  |  |
|  | Typ gniazda wejściowego ; Min. Hard Wire 3 wire (1PH+N+G), Min. Hard Wire 5-wire (3PH + N + G) |  |  |
|  | Złącza wyjściowe :Min. 1 x Hard Wire 3-wire (H N + G) |  |  |
|  | Częstotliwość wejściowa 50 Hz zgodna z wartościami zapisanymi w Polskiej Normie PN-IEC 60038 z tolerancją min. 40Hz do 70 Hz. |  |  |
|  | Urządzenie powinno zapewnić ciągłe bezprzerwowe zasilanie w trybie TRUE ON-LINE z podwójną konwersją przy zupełnych lub chwilowych zanikach napięcia i wahaniach częstotliwości w sieci elektrycznej przez cały czas pracy urządzenia. Zgodnie z normą PN-EN 62040-3. |  |  |
|  | Urządzenie musi posiadać panel komunikacyjny, w którym powinny być zainstalowane:1. port komunikacyjny USB,
2. Smart slot
3. karta sieciowa 10/100 Base-T RJ-45 (Web/SNMP).
4. RJ-45 Serial
 |  |  |
|  | Wymagana deklaracja producenta zgodności produktu z normami: EN 62040-1: 2008, EN 62040-2: 2006, oraz spełnienia dyrektyw: 2006/95/EC, 2004/108/EC. |  |  |
|  | Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia |  |  |
|  | Zasilacz musi posiadać europejskie świadectwo pochodzenia. |  |  |
|  | Czas podtrzymania min 20min przy 60% obciążenia. |  |  |

**Oprogramowanie do Inwentaryzacji aktywów i ich konfiguracji – ilość stanowisk 75**

# Zamawiający dopuszcza również rozwiązanie równoważne zgodne z poniższymi zapisami:

1. **Architektura / budowa**
	1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 75 klientów jednocześnie.
	2. **Architektura / budowa:**
		1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
		2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).
		3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.
		4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.
	3. **Konfiguracja Architektury:**
		1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.
		2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.

# Wymagania systemowe

* 1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 .
	2. Klient musi działać na systemach 32 i 64 bitowych: min. Windows Server 2019/2022, Windows 8.1/10/11.
		1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci min.: Opera, Chrome, FireFox
	3. Serwer musi działać na systemach 64 bitowych min.: m.in. Windows Server 2019/2022, Windows 8.1/10/11.

2.5. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

# Interfejsy

* 1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
	2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL
	3. System zapewnia integrację z modelem LLM.

# Funkcjonalności systemu zarządzania infrastrukturą IT

* 1. Funkcjonalność Klienta
		1. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku.
	2. Funkcjonalność konsoli administracyjnej.
		1. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.
		2. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.
	3. Funkcjonalność panelu pracownika
		1. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.
	4. Zarządzanie licencjami
		1. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.
	5. Wzorce aplikacji i pakietów
		1. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.
	6. Inwentaryzacja sprzętu komputerowego i urządzeń.
		1. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń.
	7. Inwentaryzacja urządzeń sieciowych.
		1. System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.
	8. Inwentaryzacja sprzętu.
		1. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.
	9. Ochrona danych (DLP)
		1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.
	10. Zdalna administracja komputerami
		1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.
	11. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.
	12. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.
	13. Zarządzanie Poprawkami i Aktualizacjami
		1. System musi zapewniać ciągłe monitorowanie i identyfikację brakujących aktualizacji systemowych i komponentów infrastruktury IT, oferując funkcje rozpoznawania niezainstalowanych poprawek, ich pobierania, oraz klasyfikacji. Musi umożliwiać aktualizacje bez zakłócania pracy użytkowników, zarówno zbiorowo jak i indywidualnie, z opcją szybkiego przywrócenia poprzedniego stanu systemu poprzez odinstalowanie niechcianych poprawek. System powinien również umożliwiać pomijanie niechcianych poprawek i dostarczać szczegółowe raporty dotyczące stanu aktualizacji oraz urządzeń, które mogą wymagać restartu.
	14. Zdalne Zarządzanie Zaporą (Firewall)
		1. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.
	15. Automatyzacja
		1. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.
	16. Zarządzanie magazynem IT
		1. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.
	17. Repozytorium
		1. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.
	18. Kody kreskowe
		1. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.
	19. Wysyłanie wiadomości
		1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.
	20. System musi posiadać możliwość eksportu / importu treści.
	21. Monitorowanie drukarek sieciowych i wydruków
		1. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.
	22. Monitorowanie stron www
		1. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.
	23. Monitorowanie serwerów WWW
		1. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.
	24. Monitorowanie dziennika zdarzeń
		1. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.
	25. System musi umożliwiać monitorowanie komunikatów Syslog.
	26. Monitorowanie pracy komputerów
		1. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.
	27. Monitorowanie uprawnień ACL
		1. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami.
	28. Monitorowanie sensorów
		1. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.
	29. Repozytorium CMDB
		1. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.
	30. Worktime manager
		1. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostepnienia w panelu pracownika.
	31. Raportowanie i eksport danych
		1. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.
	32. System musi zapewnić interfejs API.
		1. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.
	33. Powiadomienia
		1. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e- maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji.
	34. Bezpieczeństwo
		1. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.

# Wsparcie i pomoc

* + 1. Pomoc techniczna
			1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.
			2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.
			3. Czas trwania usługi SLA od dnia zakupu do 09.04.2026 r.

**Firewall NextGeneration – 2 szt.**

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 1 oddzielnego (fizycznego lub logicznego) 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.

System musi wspierać IPv4 oraz IPv6 w zakresie:

• Firewall.

• Ochrony w warstwie aplikacji.

• Protokołów routingu dynamicznego.

Wraz z urządzeniem należy dostarczyć 2 wkładki sfp+ SR kompatybilne do dostarczanych urządzeń.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

2. W ramach postępowania system musi zostać dostarczony w postaci pojedynczego urządzenia.

3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

4. Monitoring stanu realizowanych połączeń VPN.

5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:

• 8 portów Gigabit Ethernet RJ-45.

• 2 gniazdami SFP+ 10 Gbps.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.

4. System mieć możliwość podłączenia 2 zasilaczy . Należy dostarczyć 2 zasilacze.

Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz nie mniej niż 124 tys. nowych połączeń na sekundę.

4. Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B.

2. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.7 Gbps.

3. Wydajność szyfrowania IPSec VPN nie mniej niż 25 Gbps.

4. 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 4.5 Gbps.

5. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.2 Gbps.

6. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.2 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

2. Kontrola Aplikacji.

3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.

5. Ochrona przed atakami - Intrusion Prevention System.

6. Kontrola stron WWW.

7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

8. Zarządzanie pasmem (QoS, Traffic shaping).

9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.

12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

13. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

14. 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

• Translację jeden do jeden oraz jeden do wielu.

• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

15. 4. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.

17. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

• Amazon Web Services (AWS).

• Microsoft Azure

• Google Cloud Platform (GCP).

• OpenStack.

• VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

• Wsparcie dla IKE v1 oraz v2.

• Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).

• Obsługa protokołu Diffie-Hellman grup 19 i 20.

• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.

• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

• Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.

• Mechanizm „Split tunneling” dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

• Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

• Routingu statycznego.

• Policy Based Routingu.

• Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

3. Baza sygnatur ataków powinna zawierać minimum 1000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

2. Baza Kontroli Aplikacji powinna zawierać minimum 1000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.

6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

• ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

1. 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.

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

**W celu potwierdzenia oferowanych parametrów należy załączyć do oferty katalogi, karty informacyjne.**

**W przypadku nie spełnienia któregokolwiek z wymaganych parametrów oferta zostanie odrzucona.**