**Załącznik nr 3 - TER**

**TABELA ELEMENTÓW ROZLICZENIOWYCH - TER**

**„Dostawa sprzętu informatycznego” – GMINA ŁAGÓW**

**(wypełnia Wykonawca)**

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | **Przedmiot zamówienia** | **Cena netto łącznie** | **Cena brutto łącznie** |
| 1 | **Zakup licencji do oprogramowania antywirusowe go wraz z wdrożeniem  – 1 komplet** Producent oprogramowania:..............................................  Nazwa oprogramowania: ................................................  Rodzaj licencji:.......................................................... |  |  |
| 2 | **Zakup rozwiązania UTM dla Urzędu Gminy Łagów wraz z wdrożeniem  – 1 komplet** Nazwa Producenta:....................................................  Typ i model: ............................................................. |  |  |
| 3 | **Zakup systemu chroniącego przed wyciekiem informacji DLP wraz z licencją i wdrożeniem – 1 komplet** Producent oprogramowania: .....................................  Nazwa oprogramowania: ..............................................  Rodzaj licencji:.......................................................... |  |  |
| 4 | **Zakup oprogramowania do inwentaryzacji sprzętu i oprogramowania, monitorowania komputerów, zdalnego zarządzania komputerami z poziomu centralnej konsoli – 1 komplet** Producent oprogramowania: .....................................  Nazwa oprogramowania: ..............................................  Rodzaj licencji:.......................................................... |  |  |
| 5 | **Zakup serwera i macierzy dyskowej wraz licencją, instalacją i konfiguracją dla Urzędu Gminy Łagów – 1 komplet** Nazwa Producenta: ...........................................  Typ i model: .................................................................  **(Kryterium oceny ofert!)** Oferowany okres gwarancji: ***2 lata (minimalnie wymagany)/3 lata (punktowany)\****  ***\*niepotrzebne skreślić***  Producent typ i model zaoferowanego procesora\*: ........................................................  ***(\*wpisać w sposób umożliwiający jednoznaczne potwierdzenie spełnienia wymogów testu)***  Producent oprogramowania systemowego:....................................................  Nazwa oprogramowania systemowego: ...............................................  Rodzaj licencji oprogramowania systemowego:............................................... |  |  |
| 6 | **Zakup przełączników sieciowych wraz z instalacją i konfiguracją dla Urzędu Gminy Łagów – 2 sztuki** Nazwa Producenta:.......................................  Typ i model: .................................... |  |  |
| 7 | **Zakup systemu zasilania awaryjnego UPS na stanowiska pracy - 10 sztuk** Nazwa Producenta:...................................  Typ i model: ................................................ |  |  |
| 8 | **Zakup systemu zasilania awaryjnego UPS do serwerowni Urzędu Gminy Łagów – 1 komplet** Producent oprogramowania:....................................  Nazwa oprogramowania: ..........................................  Rodzaj licencji:.............................................................. |  |  |
| 9 | **Zakup wraz z wdrożeniem serwera do wykonywania kopii bezpieczeństwa wraz z oprogramowaniem i licencjami – 1 komplet** Nazwa Producenta:..................................  Typ i model: .............................................  Producent oprogramowania:................................  Nazwa oprogramowania: ......................................  Rodzaj licencji:...................................................... |  |  |
| 10 | **Zakup wraz z wdrożeniem serwera do zachowania logów systemowych – 1 komplet** Nazwa Producenta:........................................  Typ i model: ......................................................  Producent typ i model zaoferowanego procesora\*: ...........................................................................  ***(\*wpisać w sposób umożliwiający jednoznaczne potwierdzenie spełnienia wymogów testu)*** |  |  |
| 11 | **Usługi – 1 komplet** |  |  |
| **Razem** | |  |  |

**[DOKUMENT NALEŻY OPATRZYĆ PODPISEM ELEKTRONICZNYM, PODPISEM ZAUFANYM LUB PODPISEM OSOBISTYM]**

Oświadczamy, że zaoferowany przez nas sprzęt i oprogramowanie spełniają wszystkie minimalne wymagania Zamawiającego określone poniżej:

1. Zakup licencji do oprogramowania antywirusowe go wraz z wdrożeniem – 1 komplet

|  |
| --- |
| ***Administracja zdalna w chmurze:***   * Serwer administracyjny musi być dostępny w chmurze producenta oprogramowania antywirusowego. * Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia przechowywanych danych. * Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. * Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. * Serwer Administracyjny musi obsługiwać przynajmniej 50 000 stacji roboczych/serwerów. * 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”. * Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. * Administrator musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. * Administrator musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap. * Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android. * 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. * W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android lub równoważnym, musi istnieć możliwość jego pobrania ze sklepu z aplikacjami. * 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 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, 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. * Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie generowania raportów i usuwania stacji roboczych. 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. * Szablon grupy dynamicznej musi umożliwiać zdefiniowane przedziału czasowego kiedy grupa dynamiczna ma działać. * 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 80 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 i 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 za pośrednictwem wiadomości email. * 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 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 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 SYSLOG. * Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych. * 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: zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów. |
| ***Ochrona stacji roboczych z systemem Windows:***   * Wymagania ogólne   + Rozwiązanie musi wspierać systemy 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. * Ochrona antywirusowa i antyspyware   + 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 integrować się z Intel Threat Detection Technology (lub rozwiązaniem równoważnym).   + 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 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 programu Microsoft Outlook.   + Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu Microsoft Outlook.   + 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.   + Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.   + 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 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 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. * Ochrona przed spamem   + Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.   + 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. * Zapora osobista (personal firewall)   + 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. * Kontrola dostępu do stron internetowych   + 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. * Bezpieczna przeglądarka   + 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. |
| ***Ochrona stacji roboczych z systemem Android:***   * Wymagania ogólne   + Rozwiązanie musi wspierać system co najmniej Android 6.0.   + Rozwiązanie musi wspierać rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa.   + Rozwiązanie musi posiadać ochronę plików w czasie rzeczywistym.   + Rozwiązanie musi posiadać ochronę przed atakami typu „phishing”.   + Rozwiązanie musi skanować wszystkie typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.   + Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.   + Rozwiązanie musi posiadać ochronę proaktywną wykrywającą nieznane zagrożenia.   + W przypadku wykrycia zagrożenia użytkownik musi otrzymać odpowiednie powiadomienie.   + Rozwiązanie musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia.   + Rozwiązanie musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). * Skanowanie na żądanie:   + Rozwiązanie musi mieć możliwość skanowania zainstalowanych aplikacji.   + Informacje o skanowaniu mają być przechowywane w plikach dziennika.   + Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania.   + Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia. * Polityka ustawień:   + Administrator musi mieć wgląd w podstawowe ustawienia urządzenia, w tym co najmniej: połączenie Wi-Fi,   + GPS,   + usługi lokalizacyjne,   + pamięć,   + roaming danych,   + roaming połączeń,   + nieznane źródła,   + tryb debugowania,   + komunikacja NFC,   + szyfrowanie pamięci masowej,   + urządzenie zrootowane. * Kontrola aplikacji:   + Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji.   + Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji.   + Blokowanie aplikacji musi być możliwe w oparciu o: nazwę aplikacji,   + nazwę pakietu,   + kategorię sklepu z aplikacjami,   + uprawnienia aplikacji,   + pochodzenie aplikacji z nieznanego źródła. * Zabezpieczenia urządzenia:   + W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej: * minimalny poziom zabezpieczeń i złożoność blokady ekranu, * maksymalną dopuszczaną liczbę błędnych prób odblokowania, * odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie, * czas, po którym automatycznie nastąpi blokada ekranu, * ograniczenie dostępu do kamery wbudowanej w urządzenie. * Aktualizacje modułów:   + Rozwiązanie musi umożliwiać wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.   + Rozwiązanie musi mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje modułów co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin.   + Rozwiązanie musi posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją. * Konfiguracja i zdalne zarządzanie:   + Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne.   + Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją. |
| ***Ochrona stacji roboczych z systemem macOS:***   * Wymagania ogólne   + Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 10.12 lub nowszych.   + Rozwiązanie musi wspierać architekturę Apple Silicon (ARM)   + Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.   + Pomoc w rozwiązaniu (help) musi być dostępna co najmniej w języku polskim oraz angielskim.   + 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 funkcjonalność, która w momencie wykrycia trybu pełnoekranowego ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań.   + Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.   + Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.   + Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności).   + 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 nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.   + 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 (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.   + Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie mają być wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.   + 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.   + Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.   + Rozwiązanie musi posiadać ochronę przed atakami typu „phishing”.   + Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych. Funkcja musi umożliwiać wyłączenie dostępu do nośników: Płyta CD/DVD, Pamięć masowa, karty sieciowe, Drukarka USB, Urządzenie do tworzenia obrazów, Port szeregowy, Urządzenie przenośne. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.   + Aktualizacja silnika detekcji rozwiązania musi być dostępna z Internetu, lokalnego zasobu sieciowego lub przy pomocy serwera HTTP.   + Rozwiązanie musi posiadać możliwość pobierania aktualizacji za pośrednictwem serwera proxy.   + Rozwiązanie musi umożliwiać automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego.   + Rozwiązanie musi być wyposażone tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).   + Rozwiązanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji silnika detekcji i samego oprogramowania oraz dokonanym skanowaniu komputera.   + Rozwiązanie musi umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień.   + Rozwiązanie musi posiadać mechanizm Ochrony dostępu do stron internetowych monitoruje komunikację w ramach protokołu HTTP.   + Rozwiązanie musi pozwalać na konfigurację portów, dla których ma się odbywać skanowanie protokołu HTTP.   + Rozwiązanie musi umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy” na modyfikację konfiguracji programu.   + Rozwiązanie musi posiadać możliwość zdalnego zarządzania z poziomu Administracji zdalnej.   + 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 umożliwiać definiowanie różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.   + Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji w temacie zainfekowanej wiadomości o jej przeskanowaniu.   + Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.   + Wsparcie techniczne dla rozwiązania musi być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.   + Zapora osobista rozwiązania musi pracować w jednym z 2 trybów: * Automatyczny z wyjątkami - umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł, * Interaktywny – dla każdej nieznanej komunikacji generowane jest pytanie dla użytkownika o jej odblokowanie.   + Rozwiązanie musi mieć możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.   + Rozwiązanie musi mieć możliwość odnotowania faktu nawiązania danego połączenia w dzienniku zdarzeń.   + Rozwiązanie musi mieć możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.   + Rozwiązanie musi mieć możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla profilu: Publiczny, Praca, Dom.   + Rozwiązanie musi oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.   + Rozwiązanie musi mieć 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.   + Aktywacja stref ma się odbywać min. w oparciu o: interfejs sieciowy w systemie, Sieć WiFi, Podsieć IPv4/IPv6, Zakres adresów IPv4/IPv6, Adres IPv4/IPv6. * Kontrola dostępu do stron internetowych:   + Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli odwiedzanych stron internetowych.   + Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.   + Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.   + Reguły mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.   + Rozwiązanie musi posiadać możliwość filtrowania URL w oparciu o co najmniej 140 kategorii i podkategorii.   + Podstawowe kategorie w jakie rozwiązanie musi być wyposażona 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.   + Lista adresów URL, znajdujących się w poszczególnych kategoriach, musi być na bieżąco aktualizowana przez producenta.   + Użytkownik musi posiadać możliwość wyłączenia modułu kontroli dostępu do stron internetowych. |
| ***Ochrona serwerów z systemem zaoferowanym przez Wykonawcę:***   * Rozwiązanie musi posiadać wsparcie dla systemu operacyjnego zaoferowanego przez Wykonawcę w ramach niniejszego postępowania * 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 . * Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. |
| ***Ochrona serwerów z systemem LINUX:***   * Architektura rozwiązania   + Rozwiązanie musi posiadać skaner antywirusowy i antyspyware.   + Rozwiązanie musi umożliwiać skanowanie plików, plików spakowanych i archiwów samorozpakowujących.   + Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.   + Rozwiązanie musi posiadać wbudowany mechanizm typu ,,watchdog”. Monitoruje on tzw. stan zdrowia poszczególnych mikro-serwisów i automatycznie przeładowuje je w przypadku wykrycia zakłóceń w pracy mikro-serwisu.   + Architektura rozwiązania musi pozwalać na uruchamianie poszczególnych mikroserwisów, tylko na czas realizacji funkcjonalności przez nie realizowanych, co pozwala w znaczącym stopniu ograniczyć wykorzystanie zasobów systemu operacyjnego.   + Rozwiązanie musi wspierać wieloprocesorową i wielordzeniową architekturę, w celu zapewnienia maksymalnego zwiększenia wydajności.   + Rozwiązanie musi posiadać wsparcie dla SecureBoot-a.   + Rozwiązanie musi być wyposażone w moduł ochrony systemu plików w czasie rzeczywistym. Moduł nie może wymagać instalowania jakichkolwiek dodatkowych komponentów w systemie operacyjnym. Wszystkie komponenty muszą być instalowane w systemie, podczas instalacji z dostarczonego instalatora binarnego.   + Silnik ochrony systemu plików w czasie rzeczywistym musi stanowić dodatkowy moduł jądra systemu Linux i musi być dodawany do jądra, podczas procesu instalacji oprogramowania antywirusowego.   + Ochrona systemu plików w czasie rzeczywistym musi być zapewniona nieprzerwanie od uruchomienia produktu i obejmuje skanowanie zarówno dysków lokalnych jak i zmapowanych dysków sieciowych.   + Silnik skanujący musi działać wyłącznie z wykorzystaniem 64-bitowej architektury.   + Rozwiązanie musi być w pełni zgodne z modułem SELinux, pracującym zarówno w trybie ,,Permissive” jak i ,,Enforcing”.   + Rozwiązanie podczas procesu instalacji, musi dodawać i konfigurować własne polityki modułu SELinux, które są kompatybilne z następującymi dystrybucjami systemów Linux: Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 8, Centos 7.   + Wszystkie mechanizmy bezpieczeństwa rozwiązania muszą wspierać system informowania o zagrożeniach w czasie rzeczywistym. System ten pozwala na weryfikowanie reputacji plików oraz procesów i identyfikację nowych i nieznanych zagrożeń.   + Skaner systemu plików w czasie rzeczywistym musi działać dla operacji obsługi plików, dla co najmniej takich operacji jak: dostęp do pliku, utworzenie (zapisanie) pliku.   + Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.   + Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.   + Rozwiązanie musi być wyposażone we własny wiersz polecenia (CLI). Polecenia muszą być odpowiedzialne co najmniej za: skanowanie na żądanie, konfigurację mechanizmów bezpieczeństwa, uruchamianie aktualizacji, przeglądanie logów aplikacji, konfigurację graficznego interfejsu użytkownika, obsługę kwarantanny plików.   + Rozwiązanie musi wspierać system plików zamontowany z flagą ,,noexec”.   + Rozwiązanie musi pozwalać na uruchamianie zadań skanowania działających ,,w tle”,z możliwością ustawienia dla nich niskiego priorytetu.   + Zadania skanowania nie mogą zmieniać znacznika dostępu do plików. * Interfejs graficzny   + Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.   + Lokalna konsola administracyjna musi działać w oparciu o dynamicznie generowaną zawartość tworzoną z wykorzystaniem następujących technologii: React/Node.js, HTML5.   + Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.   + Lokalna konsola administracyjna musi zapewniać bezpieczne połączenie działające w oparciu o protokół HTTPS.   + Lokalna konsola administracyjna musi umożliwiać uruchomienie jej, na wskazanym porcie TCP.   + Logowanie do lokalnej konsoli administracyjnej musi być realizowane, poprzez podanie danych w postaci nazwy użytkownika i zdefiniowanego dla niego hasła.   + Lokalna konsola administracyjna musi zapewniać funkcjonalność zweryfikowania stanu licencji i informacji na jej temat.   + Z poziomu lokalnej konsoli administracyjnej musi być możliwość zarządzania, wbudowanym modułem menadżera kwarantanny.   + Lokalna konsola administracyjna musi zapewniać możliwość przełączenia wersji językowej konsoli, na etapie logowania. Lokalna konsola administracyjna musi posiadać interfejs, co najmniej języku: polskim, angielskim, niemieckim, francuskim, hiszpańskim, japońskim. * Skanowanie sieciowych systemów plików   + Rozwiązanie musi pozwalać na skanowanie plików składowanych i obsługiwanych przez zewnętrzne rozwiązania obsługi danych typu NAS / SAN.   + Rozwiązanie nie może wymagać instalacji jakichkolwiek dodatkowych modułów na rozwiązaniach typu NAS / SAN, a skanowanie plików musi się odbywać wyłącznie w oparciu o protokół ICAP.   + Rozwiązanie musi umożliwiać zmianę domyślnego portu protokołu ICAP.   + Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie typu Dell EMC Isilon (lub zaproponowane rozwiązanie równoważne). * Instalacja   + Rozwiązanie musi wspierać mechanizm instalacji zdalnej, realizowanej przez narzędzia do orkiestracji systemami operacyjnymi. Wspieranymi narzędziami muszą być co najmniej: Puppet, Chef, Ansible.   + Rozwiązanie musi być wyposażone w mechanizm automatycznej aktualizacji komponentów programu.   + Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.   + Rozwiązanie musi wspierać następujące systemy operacyjne: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux oraz Alma Linux. * Licencjonowanie   + Wsparcie techniczne do programu świadczone w języku polskim w języku polskim w sposób nie powodujący utraty uprawnień gwarancyjnych.   + Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji rozwiązania w trybie offline. |
| ***Szyfrowanie:***   * System szyfrowania danych musi wspierać instalację aplikacji klienckiej w posiadanym przez Zamawiającego środowisku Microsoft Windows 10 32-bit i 64-bit i Windows 11-64bit. * Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. * Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim. * Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM. * Aplikacja musi mieć możliwość korzystania z technologii TCG OPAL - dyski sprzętowo szyfrowane. * Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. * W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania. * Aplikacja do szyfrowania musi być zarządzana z poziomu konsoli webowej, wykorzystywanej do zarządzania produktem do ochrony antywirusowej. * Konsola centralnego zarządzania musi pozwalać na wygenerowanie, dla każdej zaszyfrowanej stacji, dysku ratunkowego. * Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:   + ilość znaków,   + czy hasło ma zawierać wielkie litery,   + czy hasło ma zawierać małe litery,   + czy hasło ma zawierać cyfry,   + czy hasło ma zawierać znaki specjalne,   + okres ważności,   + ilość nieudanych logowań,   + możliwość zmiany hasła. * Aplikacja musi posiadać możliwość ograniczenia wyświetlania interfejsu graficznego użytkownikom. * Administrator musi posiadać możliwość zablokowania dostępu do zaszyfrowanego dysku. |
| ***Sandbox w chmurze:***   * 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. * W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. * Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia. |
| ***Extended detection & response:***   * Serwer:   + Serwer administracyjny musi posiadać możliwość instalacji na posiadanych przez Zamawiającego systemach operacyjnych zaoferowanych przez Wykonawcę w ramach niniejszego zadania.   + 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 900 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. * Konektor:   + Pełne wsparcie dla systemu Windows 10/ Windows 11 oraz Windows Server 2012/2012R2/2016/2019/2022.   + Pełne wsparcie dla systemów Linux RHEL 7.6+/RHEL 8/RHEL 9/Ubuntu 18.04/Ubuntu 20.04/Ubuntu 22.04/Debian 10/Debian 11/Debian 12   + Wsparcie dla 32 i 64-bitowej wersji systemu Windows.   + Konektor musi współpracować z produktem antywirusowym.   + Konektor nie może działać bez produktu antywirusowego.   + W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonane przez konektor.   + Połączenie konektora do serwera zarządzającego musi być szyfrowane. * Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane. |
| ***Wsparcie techniczne:***  Oprogramowanie musi objąć ochroną 35 stanowisk i posiadać wsparcie przez okres min. 12 miesięcy (licencja na 12 miesięcy). |

1. Zakup rozwiązania UTM dla Urzędu Gminy Łagów wraz z wdrożeniem – 1 komplet

|  |
| --- |
| ***Wymagania ogólne:***   * System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. * System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. * System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. * System wspiera protokoły IPv4 oraz IPv6 w zakresie: * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. |
| ***Redundancja, monitoring i wykrywanie awarii:***   * W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. * Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. * Monitoring stanu realizowanych połączeń VPN. * System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |
| ***Interfejsy, Dysk, Zasilanie:***   * System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: * 8 portami Gigabit Ethernet RJ-45. * 2 gniazdami SFP+ 10 Gbps, obsadzonymi wkładkami 10GbE MM SR. * System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. * System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. * System jest wyposażony w zasilanie AC. * Urządzenie musi być dostarczone razem z elementami umożliwiającymi montaż w szafie Rack 19 cali. |
| ***Parametry wydajnościowe:***   * W zakresie Firewall’a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz min. 120 tys. nowych połączeń na sekundę. * Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B. * Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps. * Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 25 Gbps. * 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 Gbps. * Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2 Gbps. * Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.5 Mbps. |
| ***Funkcje Systemu Bezpieczeństwa:***  W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   * Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. * Kontrola Aplikacji. * Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. * Ochrona przed malware. * Ochrona przed atakami - Intrusion Prevention System. * Kontrola stron WWW. * Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. * Zarządzanie pasmem (QoS, Traffic shaping). * Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). * Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. * Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. * Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. * Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |
| ***Polityki, Firewall:***   * Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. * System realizuje 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. * W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. * Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. * Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. * Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. * Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. * Amazon Web Services (AWS). * Microsoft Azure. * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. * Kubernetes. |
| ***Połączenia VPN:***   * System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: * Wsparcie dla IKE v1 oraz v2. * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19, 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. * 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. * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site. * System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. |
| ***Routing i obsługa łączy WAN:***  W zakresie routingu rozwiązanie zapewnia obsługę:   * Routingu statycznego. * Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. * Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. * ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. * BFD (Bidirectional Forwarding Detection). * Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |
| ***Funkcje SD-WAN:***   * System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. * SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| ***Zarządzanie pasmem:***   * System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. * System daje możliwość określania pasma dla poszczególnych aplikacji. * System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. * System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |
| ***Ochrona przed malware:***   * Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). * Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. * System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. * System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. * System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). * Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. * System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. * Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. * Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. * Możliwość rozbudowania Systemu o dodatkową funkcjonalność wstrzymania dostarczenia pliku, dla którego jest realizowana analiza z wykorzystaniem systemu, do czasu otrzymania werdyktu z systemu |
| ***Ochrona przed atakami:***   * Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. * System chroni przed atakami na aplikacje pracujące na niestandardowych portach. * Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. * System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. * Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). * Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. * Wykrywanie i blokowanie komunikacji C&C do sieci botnet. * Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| ***Kontrola aplikacji:***   * Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. * Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. * Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. * Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. * Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). * System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |
| ***Kontrola WWW:***   * Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. * W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. * Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. * Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. * Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). * Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. * Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. * Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. * System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| ***Uwierzytelnianie użytkowników w ramach sesji:***   * System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: * 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. * System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. * System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. * Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| ***Zarządzanie:***   * Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. * Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. * Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. * System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. * System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. * Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. * Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. * Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). * Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| ***Logowanie:***   * Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. * W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. * Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. * Możliwość włączenia logowania per reguła w polityce firewall. * System zapewnia możliwość logowania do serwera SYSLOG. * Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| ***Testy wydajnościowe oraz funkcjonalne:***   * Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy. |
| ***Serwisy i licencje:***   * Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy. |
| ***Gwarancja oraz wsparcie:***   * System objęty serwisem gwarancyjnym przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu Wykonawca lub Producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| ***Wymagania dodatkowe:***   * Zamawiający wymaga, aby wsparcie serwisowe świadczyli certyfikowani inżynierowie w zakresie administracji systemami UTM, realizujący serwis w sposób nie powodujący utraty uprawnień gwarancyjnych * Przed podpisaniem umowy Wykonawca przedstawi oświadczanie o gotowości świadczenia wymaganego serwisu zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej. * Wykonawca przed podpisaniem Umowy przekaże certyfikat ISO 27001 lub równoważny na projektowanie sprzedaż i wdrażanie rozwiązań teleinformatycznych, świadczenie usług serwisowych i konsultingowych. |

1. Zakup systemu chroniącego przed wyciekiem informacji DLP wraz z licencją i wdrożeniem – 1 komplet

|  |
| --- |
| Wspierane systemy operacyjne co najmniej:   * Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi * Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi |
| Serwer administracyjny musi obsługiwać instalację na systemach oferowanych przez Wykonawcę w ramach niniejszego zadania |
| Serwer administracyjny musi obsługiwać bazy danych:   * MS SQL Server 2016 lub nowsze, * MS SQL Express, * AzureSQL S3 lub nowsze. |
| Pomoc i dokumentacja programu dostępne w języku angielskim |
| Konsola administracyjna i komunikaty klienta muszą być w języku polskim |
| Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta |
| Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych |
| Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym |
| Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia |
| Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli |
| System musi posiadać mechanizm usuwający najstarsze informacje, gdy rozmiar bazy osiągnie domyślny limit |
| Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania |
| Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu |
| Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu) |
| Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory |
| Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym |
| Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa |
| Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości e-mail oraz czynności na plikach |
| Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików |
| Administrator musi mieć możliwość filtrowania i sortowania zebranych danych |
| Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email |
| Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu |
| Serwer administracyjny musi posiadać możliwość połączenia z serwerem SMTP udostępnianym przez producenta |
| Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików |
| Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku |
| Administrator musi mieć możliwość tworzenia kategorii danych dla plików zaszyfrowanych lub dla takich gdzie zawartość pliku jest niemożliwa do odczytania |
| Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp. |
| Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, numer REGON, NIP, wyrażenia regularne, określone ciągi znaków i numer IBAN. |
| Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym |
| Administrator musi mieć możliwość wyszukiwania danych wrażliwych w zasobach lokalnych |
| Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM |
| Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP |
| Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania |
| System musi ochraniać pocztę e-mail, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników |
| System musi ochraniać pliki w, kontrolując aktywność plików w SharePoint, OneDrive i Teams |
| System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach |
| System musi umożliwiać synchronizacji grup bezpieczeństwa z Active Directory na potrzeby logowania do konsoli zarządzającej |
| System musi umożliwiać administratorowi nadanie użytkownikowi uprzywilejowanego dostępu, przez co nie będzie obejmowany politykami przez określony czas – 1 godzinę, 6 godzin lub do końca dnia |
| System musi posiadać możliwość tworzenia polityk dynamicznych, pozwalających na dostosowywanie się akcji (takich jak zapisywanie logu, powiadomienie użytkownika, blokowanie lub blokowanie z możliwością zastąpienia przez użytkownika) w zależności od profilu pracy użytkownika wykonującego daną czynność, gdzie akcja dobierana jest w zależności od wyniku systemu uczenia maszynowego |
| System musi umożliwiać dostosowanie polityk dynamicznych do dwóch trybów: standardowy oraz łagodny. Możliwość taka musi istnieć per użytkownik |
| System musi umożliwiać tworzenie raportów na podstawie logów zebranych w układach danych z możliwością dostosowania filtrów, użytkowników oraz zakresu czasu objętych raportowaniem |
| System musi umożliwiać utworzenie raportu, który będzie zawierał podsumowanie stanu zabezpieczenia danych wraz z rekomendacjami w formie cyklicznej |
| System musi zbierać informacje na temat podłączanych urządzeń do komputera, odwiedzanych domen internetowych, ścieżek sieciowych, drukarek lokalnych oraz sieciowych, umożliwiając jednocześnie przypisanie takowych wpisów do bezpiecznych lub niezaufanych lokalizacji bez potrzeby manualnego wpisywania ścieżek lub numerów seryjnych urządzeń |
| Dla każdej z wyżej wymienionych lokalizacji system powinien umożliwiać przypisanie indywidualnej polityki dostępu – np. umożliwiając przesyłanie danych do lokalizacji oznaczonej jako bezpieczna, jednocześnie blokując wysyłkę do lokalizacji oznaczonej jako niezaufana lub nieprzypisana |
| System musi umożliwiać audyt operacji wykonywanych przez administratora w obszarze konsoli DLP |
| System musi umożliwiać podłączenie archiwa logów w formacie plików o rozszerzeniu mdf |
| System powinien umożliwiać monitoringi ochronę 35 stacji roboczych oraz posiadać wsparcie na okres min. 12 miesięcy |

1. Zakup oprogramowania do inwentaryzacji sprzętu i oprogramowania, monitorowania komputerów, zdalnego zarządzania komputerami z poziomu centralnej konsoli – 1 komplet

|  |
| --- |
| ***MONITOROWANIE INFRASTRUKTURY***  Bezagentowy monitoring serwerów Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:   * wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping * wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU) * wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci * wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki * wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła. * wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku * wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze * wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie * wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny * zablokowania mapy urządzeń przed przypadkową edycją * serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów * serwerów pocztowych: * program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty * program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem) * program ma możliwość wykonywania operacji testowych * program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa * monitorowania serwerów WWW i adresów URL * cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS * obsługi szyfrowania TLS w powiadomieniach e-mail * obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID * obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych * monitoringu routerów i przełączników wg: * zmian stanu interfejsów sieciowych * ruchu sieciowego * podłączonych stacji roboczych – graficzna prezentacja panelu switcha * ruchu generowanego przez podłączone do portów stacje robocze * serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie * wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu * monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano * zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny * wydajności systemów Windows: * obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy   Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program posiada również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.  Program umożliwia również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams (poprzez mechanizmy webhook i workflow) oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy pozwalają na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie umożliwia wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0 |
| ***INWENTARYZACJA ZASOBÓW:***   * Program automatycznie gromadzi informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz: * Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp. * Umożliwia odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe. * Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. * Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. * Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. * Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. * Umożliwia odczytanie numeru seryjnego (klucze licencyjne). * Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. * Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. * Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). * Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane. * Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania: * przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, * przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów, * tworzenia powiązań między zasobami a urządzeniami, * tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych, * tworzenia relacji pomiędzy zasobami, * wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy, * definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz, * określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, * określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, * masową edycję atrybutów zasobów, * definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, * importu danych z zewnętrznego źródła (.CSV), * przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., * kopiowanie powielanie zasobów z możliwością wyboru atrybutów do powielenia, * automatyczne nadawanie numeru inwentarzowego do powielanych zasobów, * tworzenia powiązań między zasobami a dokumentami w relacji 1:N, * oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., * ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, * generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, * przygotowania wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, * konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, * konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, * archiwizacji i porównywania audytów zasobów, * tworzenia kodów kreskowych dla zasobów, * drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, * inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet, * możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android, * inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), * definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”) * powiązania zgłoszeń w module pomocy użytkownikom z zasobami. * Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez: * Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. * Informacje o aplikacjach używanych w organizacji. * Tworzenie własnych wzorców aplikacji. * Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. * Informacje o komputerach, na których aplikacja została wykryta. * Zarządzanie posiadanymi licencjami. * Wskazywanie osób odpowiedzialnych za licencję. * Wskazanie użytkowników licencji. * Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. * Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu. * Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych. * Zarządzanie posiadanymi licencjami: raport zgodności licencji. * Możliwość przypisania do programów numerów seryjnych, wartości itp. * Okna audytowe posiadają możliwość filtrowania elementów per oddział. |
| ***Licencja:***  Dostarczona licencja musi umożliwiać na monitorowanie, inwentaryzowanie min. 35 urządzeń i posiadać wsparcie przez okres 12 miesięcy. |

1. Zakup serwera i macierzy dyskowej wraz licencją, instalacją i konfiguracją dla Urzędu Gminy Łagów – 1 komplet

|  |
| --- |
| ***Obudowa:***   * Obudowa Rack o wysokości max 2U * 8 slotów na dyski 2.5” * Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| ***Płyta główna:***   * Płyta główna z możliwością zainstalowania jednego procesora. * Obsługa procesorów 144 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinny znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. * Płyta główna powinna obsługiwać do 4TB pamięci RAM. |
| ***Chipset:***   * Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych. |
| ***Procesor:***   * Zainstalowany jeden procesor min. 12-rdzeniowy, min. 2.2GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 158 w teście SPECspeed 2017\_fp\_base, dostępnym na stronie www.spec.org dla konfiguracji jednoprocesorowej oferowanego serwera. |
| ***Pamięć RAM:***   * 4x 32GB DDR5 RDIMM 6400MT/s, |
| ***Kontroler RAID:***   * Min. 8GB nieulotnej pamięci cache, * Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. * Wsparcie dla dysków samoszyfrujących * Obsługa dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS |
| ***Dyski twarde:***   * 6 dysków SAS o pojemności min. 2.4TB Hot-Plug |
| ***Gniazda PCI:***   * Dwa sloty PCIe x16 FH generacji 5 |
| ***Karty sieciowe:***   * 4 interfejsy sieciowe 1Gb Ethernet w standardzie Base-T (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) * 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) obsadzone wkładkami SR MM 10/25GbE |
| ***Wbudowane porty:***   * 3 porty USB w tym min: * 1 port USB 2.0 Type-C * 2 porty USB 3.1 * Port VGA z tyłu obudowy |
| ***Video:***   * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| ***Zasilacze:***   * Redundantne, Hot-Plug min. 800W klasy Titanium |
| ***Elementy montażowe:***   * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych * Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych |
| ***Bezpieczeństwo:***   * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 V3 * Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem * Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). Wymagane dołączenie przed podpisaniem Umowy oświadczenia potwierdzającego spełnienie powyższych zaleceń. |
| ***Karta zarządzania:***  Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika * możliwość podmontowania zdalnych wirtualnych napędów * wirtualną konsolę z dostępem do myszy, klawiatury * wsparcie dla IPv6 * wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer * integracja z Active Directory * możliwość obsługi przez sześciu administratorów jednocześnie * Wsparcie dla automatycznej rejestracji DNS * wsparcie dla LLDP * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej * możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. * Monitorowanie zużycia dysków SSD * Automatyczne zgłaszanie alertów do centrum serwisowego * Automatyczne update firmware dla wszystkich komponentów serwera * Możliwość przywrócenia poprzednich wersji firmware * Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON * Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych * Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. * Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera * kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania * możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień * możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera * możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer * możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe   Możliwość rozszerzenia funkcjonalności o:   * możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch * możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej * Automatyczne odświeżanie certyfikatów SSL * monitorowanie przepływu powietrza na bieżąco (w CFM) |
| ***Oprogramowanie do zarządzania:***  Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych * integracja z Active Directory * Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta * Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish * Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram * Szczegółowy opis wykrytych systemów oraz ich komponentów * Możliwość eksportu raportu do CSV, HTML, XLS, PDF * Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. * Grupowanie urządzeń w oparciu o kryteria użytkownika * Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji * Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * Szybki podgląd stanu środowiska * Podsumowanie stanu dla każdego urządzenia * Szczegółowy status urządzenia/elementu/komponentu * Generowanie alertów przy zmianie stanu urządzenia. * Filtry raportów umożliwiające podgląd najważniejszych zdarzeń * Integracja z service desk producenta dostarczonej platformy sprzętowej * Możliwość przejęcia zdalnego pulpitu * Możliwość podmontowania wirtualnego napędu * Kreator umożliwiający dostosowanie akcji dla wybranych alertów * Możliwość importu plików MIB * Przesyłanie alertów „as-is” do innych konsol firm trzecich * Możliwość definiowania ról administratorów * Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów * Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) * Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta * Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów * Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. * Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. * Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile * Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. * Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. * Zdalne uruchamianie diagnostyki serwera. * Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. * Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| ***Oprogramowanie do monitorowania:***  Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:   * Monitoring: * ilość podłączonych oraz rozłączonych systemów * stan podłączonych urządzeń * informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów * Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia * informacje o statusie gwarancji dla poszczególnych urządzeń * informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń * informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. * Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych * Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. * Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. * Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. * Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. * Monitoring parametrów serwerów z informacją o minimum: * Obciążeniu procesora * Zużyciu pamięci RAM * Temperaturze procesorów * Temperaturze powietrza wlotowego * Zużyciu prądu * Zmianach w fizycznej konfiguracji serwera * Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. * Monitoring parametrów pamięci masowych z informacją o minimum: * Opóźnieniach * IOPS * Przepustowości * Utylizacji kontrolerów * Pojemność całkowita i dostępna * Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. * Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. * Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata * Informacje o poziomie redukcji danych * Informacje o statusie replikacji oraz snapshotów * Monitoring parametrów przełączników sieciowych z informacją o minimum: * Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny * Stanie komponentów: zasilacze, wentylatory * Podłączonych hostach * Ilości i statusu portów * Utylizacji procesora * Utylizacji poszczególnych portów * Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. * Aktualizacja firmware * możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania * możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania * możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania * możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania * możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania * Raporty * Możliwość generowania raportów dla serwerów zawierających informację o: * Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej * Średnim obciążeniu: procesorów, pamięci RAM, IO, * Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: * Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji * Generowanie raportów do plików CSV i PDF * Cyberbezpieczeństwo * Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. * Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. * Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. * Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. * Wspierane urządzenia * Urządzenia dostarczane w ramach postępowania * Wirtualny asystent * Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; * Możliwość rozszerzenia funkcjonalności * Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. * Inne * Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android |
| ***Certyfikaty:***   * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 (lub normami równoważnymi) * Serwer musi posiadać deklaracja CE. * Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży przed podpisaniem Umowy dokument potwierdzający spełnianie wymogu. |
| ***Dokumentacja użytkownika:***   * Zamawiający wymaga dokumentacji w języku polskim lub angielskim. * Możliwość telefonicznego lub internetowego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela |
| ***Warunki gwarancji:***   * Zamawiający wymaga zapewnienia gwarancji z zakresu wdrażanej technologii na okres 2 lat (minimalnie wymagane) – **Wykonawca może zaoferować wiążący dla niego 3 -letni okres gwarancji – kryterium oceny ofert o wadze 40%** * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania, w tym także sprzedanego oprogramowania. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Technik z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. * Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę i nie może powodować utraty uprawnień gwarancyjnych. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. * Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia (przed podpisaniem umowy), że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy przekazać przed podpisaniem Umowy * Ze względu na bezpieczeństwo danych Wykonawca musi posiadać certyfikat ISO-27001 (lub równoważny) na projektowanie, sprzedaż i wdrażanie rozwiązań teleinformatycznych – dokumenty potwierdzające należy przekazać przed podpisaniem Umowy |
| ***System operacyjny:***  Wraz z serwerem należy dostarczyć system operacyjny Windows Server 2025 Standard (lub równoważny pod kątem posiadanych funkcjonalności) wraz z 35 licencjami dostępowymi dla użytkowników |

1. Zakup przełączników sieciowych wraz z instalacją i konfiguracją dla Urzędu Gminy Łagów – 2 sztuki

|  |
| --- |
| ***Parametry fizyczne platformy:***   * Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. * Zasilanie AC 230V. * Maksymalny pobór mocy: 45 W. * Minimalny zakres temperatury pracy: 0-40ᵒC. |
| ***Interfejsy sieciowe:***   * 24 porty 2.5G/1G RJ-45. * 6 portów 10G/1G SFP+/SFP obsadzone wkładkami SFP+ 10GbE MM SR. |
| ***Zarządzanie:***   * Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. * Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). * Wsparcie dla SNMP w wersjach 1-3 * Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. * Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. * Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. * Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). * Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. * Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. * Automatycznie wykonywane rewizje konfiguracji. |
| ***Parametry wydajnościowe:***   * Przepustowość urządzenia - min. 240 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 350 Mpps. * Tablica adresów MAC o pojemności co najmniej 32k wpisów. * Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund. |
| ***Wymagane funkcje:***   * Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. * Obsługa Jumbo Frames. * Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). * Agregacja portów zgodna ze standardem 802.3ad. * Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. * Obsługa routingu statycznego. * Port-mirroring. * Uwierzytelnianie 802.1x na poziomie portu. * Uwierzytelnianie 802.1x w oparciu o adres MAC. * W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). * W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. * W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. * Obsługa protokołu sFlow. |
| ***Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC:***   * Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: * Centralne zarządzanie konfiguracją urządzenia * Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania * Centralne zarządzanie sieciami VLAN. * Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u * Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. * Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. * Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. * Automatyczna detekcja i rekomendacje konfiguracji. * Przesyłanie logów na zewnętrzny serwer syslog. * Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. * Obsługa białych i czarnych list adresów MAC. * Wykrywanie aplikacji komunikujących się w sieci. * Musi być możliwe redundantne połączenie z elementami zarządzającymi. * W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC. |
| ***Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa:***   * System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. * System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing. |
| ***Gwarancja oraz wsparcie:***   * System musi być objęty serwisem gwarancyjnym przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w sposób nie powodujący utraty uprawnień gwarancyjnych. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| ***Dodatkowe wymagania:***   * W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca winien przedłożyć przed podpisaniem Umowy 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. |
| ***Wymagania ilościowe:***   * W ramach postępowania należy dostarczyć dwie sztuki przełączników. |

1. Zakup systemu zasilania awaryjnego UPS na stanowiska pracy

|  |
| --- |
| ***Dane ogólne:***   * Moc wyjściowa (pozorna / czynna): 850 VA / 550 W * Topologia: VI (line interactive) * Typ obudowy: Tower |
| ***Wejście:***   * Napięcie znamionowe (wartość skuteczna): 230 V AC * Zakres napięcia wejściowego (wartości skuteczne) i tolerancja: ~162 ÷ 290 V ± 7 V * Częstotliwość znamionowa napięcia wejściowego: 50 / 60 Hz (autodetekcja) * Zakres częstotliwości i tolerancja: 40 ÷ 70 Hz ± 1 Hz * Progi przełączania: sieć – UPS: ~162÷ 290 V ± 7 V |
| ***Wyjście:***   * Napięcie znamionowe (wartość skuteczna): 230 V AC * Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja - praca sieciowa: ~191 ÷ 253 V ± 7 V * Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja - praca rezerwowa: ~230 V ± 10 % * Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej): Schodkowa aproksymacja sinusoidy / Tak jak na wejściu * Częstotliwość znamionowa napięcia wyjściowego: 50 / 60 Hz * Zakres częstotliwości (tolerancja) - praca rezerwowa: 50 / 60 Hz ± 1% * Progi przełączania: UPS – sieć: ~172 ÷ 280 V ± 7 V * Czas przełączenia na pracę rezerwową: < 6 ms * Czas powrotu na pracę sieciową: 0 ms |
| ***Akumulatory i czasy podtrzymania:***   * Akumulatory wewnętrzne: minimum 2 x 12 V / 5 Ah VRLA * Dopuszczalna całkowita pojemność akumulatorów wewnętrznych: 5 Ah * Czas podtrzymania z baterii wewnętrznych (100 % / 80 % / 50 % Pmax): min. 1,5 / 3 / 8 min * Maksymalny czas ładowania baterii wewnętrznych UPS - po 80% wyładowaniu baterii: 8 h |
| ***Zabezpieczenia:***   * Zabezpieczenie wejściowe: * Przeciwzwarciowe - Bezpiecznik automatyczny * Przeciwprzepięciowe * Zabezpieczenie wyjściowe: * Elektroniczne – przeciwzwarciowe i przeciążeniowe |
| ***Wyposażenie i funkcje dodatkowe:***   * Przyłącza wyjściowe (liczba i typ gniazd): minimum 6 x IEC * Sygnalizacja: Akustyczno – optyczna * Interfejsy komunikacyjne: USB HID |
| ***Gwarancja i serwis:***   * min 24 miesięcy na elektronikę i 12 miesiące na akumulatory; * serwis realizowany w systemie door to door |
| ***Wymagania ilościowe:***   * W ramach postępowania należy dostarczyć dziesięć sztuk urządzeń. |

1. Zakup systemu zasilania awaryjnego UPS do serwerowni Urzędu Gminy Łagów – 1 komplet

|  |
| --- |
| ***Dane ogólne:***   * Moc wyjściowa (pozorna/czynna): 6kVA/6KW * Topologia: online * Liczba faz napięcia (wejście / wyjście): 1/1 * Typ obudowy: Rack / Tower * Sprawność max (dla VFI): 95% * Sprawność (dla ECO): ≥ 98 % * Wilgotność względna w czasie pracy: < 95% (bez kondensacji) * Stopień ochrony: IP20 |
| ***Wejście:***   * Napięcie znamionowe (wartość skuteczna): 230 V AC * Zakres napięcia wejściowego (wartości skuteczne): 110 ÷ 275 V AC ± 3% * Prąd znamionowy: 27,4 A * Częstotliwość znamionowa napięcia wejściowego: 50 / 60 Hz * Zakres częstotliwości i tolerancja: 45 ÷ 55 / 54 ÷ 66 ±1 Hz * Współczynnik mocy PF: ≥0,99 * Współczynnik odkształceń prądu wejściowego THDi: < 3 % |
| ***Wyjście:***   * Napięcie znamionowe (wartość skuteczna): 230 V AC * Zakres napięcia wyjściowego (wartości skuteczne): 220 V AC / 230 V AC / 240 V AC ± 1 % * Kształt napięcia wyjściowego: Sinusoidalny * Zakres częstotliwości (tolerancja): 50 / 60 ± 0,1 Hz * Współczynnik odkształceń napięcia wyjściowego THDu: * < 1 % dla Pmax (liniowe) * < 5 % (nieliniowe wg PN-EN 62040-3) * Czas przełączenia na pracę rezerwową: 0 ms * Czas powrotu na pracę sieciową: 0 ms |
| ***Akumulatory i czasy podtrzymania:***   * Akumulatory modułu bateryjnego: 12 V / 9 Ah VRLA * Liczba akumulatorów modułu bateryjnego: minimum 1 x 20 * Dopuszczalna całkowita pojemność akumulatorów modułu bateryjnego: 9 Ah * Maksymalna liczba modułów bateryjnych: 6 * Czas podtrzymania (100% / 80% / 50% Pmax): minimum 7 / 10 / 19 min * Napięcie nominalne obwodu DC: 240 V DC * Maksymalny czas ładowania baterii 1 modułu bateryjnego - po 80% wyładowaniu baterii: ≤ 3 h |
| ***Zabezpieczenia:***   * Wejściowe: * Przeciwprzepięciowe * Wyjściowe: * Praca falownikowa – elektroniczne zwarciowe i przeciążeniowe * Przeciwzwarciowe – zabezpieczenie gniazd wyjściowych IEC 320 C13 * Zabezpieczenia DC (zewnętrzny moduł bateryjny): * Zabezpieczenie nadprądowe |
| ***Wyposażenie i funkcje dodatkowe:***   * należy dostarczyć wszystkie niezbędne elementy do montażu w szafie RACK * złącza wyjściowe: minimum 2x IEC 320 C13 (10 A) * EPO * Sygnalizacja: Akustyczno – optyczna; graficzny wyświetlacz LCD, diody LED * Interfejsy komunikacyjne: RS232, USB HID, styki bezpotencjałowe: 1x wejściowe, 1x wyjściowe * wymagana sieciowa karta zarządzająca SNMP / http * Wymagane oprogramowanie monitorująco-zarządzające |
| ***Gwarancja i serwis:***   * min 36 miesięcy na elektronikę i 12 miesiące na akumulatory; * serwis realizowany w systemie door to door |

1. Zakup wraz z wdrożeniem serwerów do wykonywania kopii bezpieczeństwa wraz z oprogramowaniem i licencjami

|  |
| --- |
| ***Procesor:***   * Architektura 64 bitowa * Ilość rdzeni – minimum 4 * Częstotliwość pracy – minimum 1,7GHz |
| ***Pamięć RAM:***   * Zainstalowane min. 4 GB * Obsługa do 16GB |
| ***Pamięć FLASH:***   * Minimum 512MB |
| ***Dyski twarde:***   * Obsługa minimum 8 dysków bez konieczności rozbudowy * Obsługa dysków 2,5” oraz 3,5” * Obsługa dysków o pojemności do min. 22TB * Zainstalowane 8 dysków o pojemności 20TB każdy |
| ***Porty sieciowe:***   * 2 porty 2,5GbE Base-T * 2 porty 10GbE SFP+ obsadzone wkładkami 10GbE MM SR * Możliwość podłączenia karty WLAN do portu USB |
| ***Porty USB:***   * 4 porty USB 3.2 |
| ***Obudowa:***   * Wysokość 2U * Diody: status, lan, hdd * Przyciski: zasilanie, reset * Szyny do montażu w szafie rack |
| ***Zasilanie:***   * Dwa zasilacze o mocy 250W każdy |
| ***Obsługiwane systemy plików:***   * Dyski wewnętrzne: EXT4 * Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+ |
| ***Szyfrowanie wolumenów:***   * Min. AES 256 |
| ***Zarządzanie dyskami:***   * Pojedynczy Dysk, 0, 1, 5, 6, 10, 50, 60, JBOD, * Obsługa Hot Spare per grupa RAID oraz global hot spare * Rozszerzanie pojemności Online RAID * Migracja poziomów Online RAID * HDD S.M.A.R.T. * Skanowanie uszkodzonych bloków (pliku) * Przywracanie macierzy RAID * Obsługa map bitowych * Pula pamięci masowej * Obsługa migawek woluminów i LUN blokowych * Obsługa replikacji migawek |
| ***Wbudowana obsługa iSCSI:***   * Multi-LUN na Target * Obsługa LUN Mapping & Masking * Obsługa MPIO * Migawka LUN * Kopia zapasowa iSCSI LUN |
| ***Zarządzanie prawami dostępu:***   * Ograniczenie dostępnej pojemności dysku dla użytkownika * Importowanie listy użytkowników * Zarządzanie kontami użytkowników * Zarządzanie grupą użytkowników * Zarządzanie współdzieleniem w sieci * Tworzenie użytkowników za pomocą makr * Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL |
| ***Obsługa Windows AD:***   * Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web * Funkcja serwera LDAP |
| ***Funkcje backup:***   * Oprogramowanie do tworzenia kopii bezpieczeństwa urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde, |
| ***Współpraca z zewnętrznymi dostawcami usług chmury (co najmniej):***   * Google Drive, * Dropbox, * Microsoft OneDrive, * Microsoft OneDrive for Business i Box |
| ***Darmowe aplikacje na urządzenia mobilne:***   * Monitoring i zarządzanie urządzeniem * Synchronizacja plików * Obsługa kamer * Dostępne na systemy iOS oraz Android |
| ***Obsługiwane serwery:***   * Serwer plików * Serwer FTP * Serwer WEB * Serwer kopii zapasowych * Serwer multimediów UPnP * Serwer pobierania (Bittorrent / HTTP / FTP) * Serwer Monitoringu |
| ***VPN:***   * VPN client / VPN server * Obsługa PPTP * OpenVPN |
| ***Administracja systemu:***   * Połączenia HTTP/HTTPS * Powiadamianie przez e-mail (uwierzytelnianie SMTP) * Powiadamianie przez SMS * Ustawienia inteligentnego chłodzenia * DDNS oraz zdalny dostęp w chmurze * SNMP (v2 & v3) * Obsługa UPS z zarządzaniem SNMP (USB) * Obsługa sieciowej jednostki UPS * Monitor zasobów * Kosz sieciowy dla CIFS/SMB oraz AFP * Monitor zasobów systemu w czasie rzeczywistym * Rejestr zdarzeń * System plików dziennika * Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line * Aktualizacja oprogramowania * Ustawienia: Back up, przywracania, resetowania systemu |
| ***Konteneryzacja:***   * Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker |
| ***Zabezpieczenia:***   * Filtracja IP * Ochrona dostępu do sieci z automatycznym blokowaniem oraz blokowanie na podstawie Geolokalizacji * Połączenie HTTPS * FTP z SSL/TLS (Explicit) * Obsługa SFTP (tylko admin) * Szyfrowanie AES 256-bit * Szyfrowana zdalna replikacja (Rsync poprzez SSH) * Import certyfikatu SSL * Powiadomienia o zdarzeniach za pośrednictwem Email i SMS |
| ***Możliwość instalacji dodatkowego oprogramowania:***   * Sklep z aplikacjami * Instalacja z paczek |
| ***Gwarancja:***   * 36 miesięcy |

1. Zakup wraz z wdrożeniem serwera do zachowania logów systemowych

|  |
| --- |
| ***Obudowa:***   * Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3.5” |
| ***Płyta główna:***   * Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i identyfikująca producenta pod kątem graficznym/opisowym (np. tabliczka znamionowa/logo, naklejka etc) * Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci |
| ***Chipset:***   * Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych |
| ***Procesor:***   * Zainstalowany jeden procesor min. 6-rdzeniowy, min. 3.1GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 71 w teście SPECspeed2017\_fp\_base, dostępnym na stronie www.spec.org dla konfiguracji jednoprocesorowej oferowanego serwera. |
| ***Pamięć RAM:***   * 2x 32GB pamięci RAM DDR5 UDIMM o częstotliwości pracy 5600MT/s. |
| ***Karta graficzna:***   * Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200 |
| ***Wbudowane porty:***   * min. 3 porty USB w tym 1 port USB 3.0 z tyłu obudowy, * 1 port VGA na tylnym panelu, * 1 port RS232 |
| ***Interfejsy sieciowe:***   * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie Base-T |
| ***Kontroler RAID:***   * Min. 8GB nieulotnej pamięci cache, * Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10. * Wsparcie dla dysków samoszyfrujących |
| ***Dyski twarde:***   * Zainstalowane 4 dyski SAS o pojemności min. 16TB, Hot-Plug. * Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |
| ***Zasilacze:***   * Redundantne, o mocy maks. 700W klasy Titanium |
| ***Bezpieczeństwo:***   * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| ***Elementy montażowe:***   * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych * Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych |
| ***Karta zarządzania:***  Zainstalowana niezależna karta zarządzająca od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; * możliwość podmontowania zdalnych wirtualnych napędów; * wirtualną konsolę z dostępem do myszy, klawiatury; * wsparcie dla IPv6; * wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; * integracja z Active Directory; * możliwość obsługi przez dwóch administratorów jednocześnie; * wsparcie dla dynamic DNS; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. * możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera * możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera   oraz z możliwością rozszerzenia funkcjonalności o:   * Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej * Przesyłanie danych telemetrycznych w czasie rzeczywistym * Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze * Automatyczna rejestracja certyfikatów (ACE) |
| ***Oprogramowanie do zarządzania:***  Możliwość zainstalowania oprogramowania do zarządzania, spełniającego poniższe wymagania:   * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych * integracja z Active Directory * Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta * Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish * Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram * Szczegółowy opis wykrytych systemów oraz ich komponentów * Możliwość eksportu raportu do CSV, HTML, XLS, PDF * Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. * Grupowanie urządzeń w oparciu o kryteria użytkownika * Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji * Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * Szybki podgląd stanu środowiska * Podsumowanie stanu dla każdego urządzenia * Szczegółowy status urządzenia/elementu/komponentu * Generowanie alertów przy zmianie stanu urządzenia. * Filtry raportów umożliwiające podgląd najważniejszych zdarzeń * Integracja z service desk producenta dostarczonej platformy sprzętowej * Możliwość przejęcia zdalnego pulpitu * Możliwość podmontowania wirtualnego napędu * Kreator umożliwiający dostosowanie akcji dla wybranych alertów * Możliwość importu plików MIB * Przesyłanie alertów „as-is” do innych konsol firm trzecich * Możliwość definiowania ról administratorów * Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów * Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) * Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta * Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów * Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. * Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. * Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile * Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. * Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. * Zdalne uruchamianie diagnostyki serwera. * Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. * Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| ***Oprogramowanie do monitorowania:***  Oparta na chmurze aplikacja oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:   * Monitoring: * ilość podłączonych oraz rozłączonych systemów * stan podłączonych urządzeń * informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów * Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia * informacje o statusie gwarancji dla poszczególnych urządzeń * informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń * informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. * Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych * Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. * Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. * Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. * Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. * Monitoring parametrów serwerów z informacją o minimum: * Obciążeniu procesora * Zużyciu pamięci RAM * Temperaturze procesorów * Temperaturze powietrza wlotowego * Zużyciu prądu * Zmianach w fizycznej konfiguracji serwera * Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. * Monitoring parametrów pamięci masowych z informacją o minimum: * Opóźnieniach * IOPS * Przepustowości * Utylizacji kontrolerów * Pojemność całkowita i dostępna * Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. * Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. * Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata * Informacje o poziomie redukcji danych * Informacje o statusie replikacji oraz snapshotów * Monitoring parametrów przełączników sieciowych z informacją o minimum: * Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny * Stanie komponentów: zasilacze, wentylatory * Podłączonych hostach * Ilości i statusu portów * Utylizacji procesora * Utylizacji poszczególnych portów * Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. * Aktualizacja firmware * możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania * możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania * możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania * możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania * możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania * Raporty * Możliwość generowania raportów dla serwerów zawierających informację o: * Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej * Średnim obciążeniu: procesorów, pamięci RAM, IO, * Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: * Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji * Generowanie raportów do plików CSV i PDF * Cyberbezpieczeństwo * Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. * Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. * Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. * Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. * Wspierane urządzenia * Urządzenia dostarczane w ramach postępowania * Wirtualny asystent * Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; * Możliwość rozszerzenia funkcjonalności * Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. * Inne * Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android |
| ***Certyfikaty:***   * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub zgodnie z normami równoważnymi * Serwer musi posiadać deklaracja CE. * Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami rozporządzenia nr 1272/2008WE. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży przed podpisaniem Umowy dokument potwierdzający spełnianie wymogu. |
| ***Dokumentacja użytkownika:***   * Zamawiający wymaga dokumentacji w języku polskim lub angielskim. * Możliwość telefonicznego lub internetowego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| ***Warunki gwarancji:***   * Zamawiający wymaga zapewnienia gwarancji z zakresu wdrażanej technologii na okres 36 miesięcy z czasem reakcji następny dzień roboczy. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania, w tym także sprzedanego oprogramowania. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Technik z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. * Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. * Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: * Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. * Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. * Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. * Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. * Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. * Wymagane dołączenie przed podpisaniem Umowy oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta lub we współpracy z autoryzowanym partnerem serwisowym producenta. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 (lub równoważne) na świadczenie usług serwisowych oraz świadczyć naprawy/serwis w sposób nie powodujący utraty gwarancji. – dokumenty potwierdzające należy przekazać przed podpisaniem Umowy * Ze względu na bezpieczeństwo danych Wykonawca musi posiadać certyfikat ISO-27001 (lub równoważne) na projektowanie, sprzedaż i wdrażanie rozwiązań teleinformatycznych – dokumenty potwierdzające należy przekazać przed podpisaniem Umowy |
| ***Dodatkowe wymagania:***   * Zamawiający wymaga instalacji na dostarczanym serwerze oprogramowania do zbierania logów, oraz o ile to możliwe konfiguracji wszystkich dostarczanych w ramach tego postępowania urządzeń w celu przesyłania logów. |

1. Usługi

|  |
| --- |
| W ramach postępowania Wykonawca zobowiązany jest do: |
| * opracowania projektu wdrożeniowego obejmującego instalację i konfigurację rozwiązań |
| * dostarczenia sprzętu i oprogramowania do wskazanej lokalizacji |
| * przeniesienia własności na urządzenia oraz gwarancje, udostępnienia licencji niezbędnych do uruchomienia sprzętu i oprogramowania, |
| * montażu i konfiguracji urządzeń we wskazanym miejscu w szafie RACK. Wymagane jest aby usługa montażu była wykonana z zachowaniem należytej staranności i przestrzeganiem przepisów BHP. Okablowanie sieciowe powinno być opisane tak aby możliwa była identyfikacja połączeń, |
| * instalacji i konfiguracji dostarczanego oprogramowania w oparciu o projekt wdrożeniowy oraz przygotowanie dokumentacji powdrożeniowej wraz ze schematami graficznymi wdrożonego rozwiązania, |
| * wykonania prac wdrożeniowych obejmujących:   + fizycznej instalacji dostarczanych urządzeń z uwzględnieniem redundancji połączeń   + aktualizacja systemów operacyjnych na dostarczanych serwerach,   + aktualizacja sterowników, firmware itp. na dostarczanych urządzeniach   + przygotowania segmentacji sieci Zamawiającego zgodnie z projektem wdrożeniowym   + dostosowanie polityk Firewall do potrzeb wdrażanego rozwiązania,   + budowa systemu backup z wykorzystaniem dostarczanego serwera backup   + instalacja i konfiguracja oprogramowania antywirusowego   + instalacja i konfiguracja oprogramowania DLP   + instalacja i konfiguracja oprogramowania do inwentaryzacji i monitorowania   + instalacja i konfiguracja oprogramowania do przechowywania logów (logi muszą być o ile to możliwe zbierane ze wszystkich dostarczanych urządzeń). |
| * przeprowadzenia szkolenia pracowników w zakresie zarządzania, administrowania i działania w ramach dostarczonych rozwiązań, |
| * zapewnienia pomocy technicznej eksperta, |
| * dostarczenia wszystkich niezbędnych materiałów instalacyjnych (przewodów, wkładek światłowodowych) do realizacji przedmiotu zamówienia |