**Opis przedmiotu zamówienia**

Przedmiotem Zamówienia jest dostarczenie urządzeń, licencji oraz wdrożenie, konfiguracja urządzeń i oprogramowania w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych w zakresie cyberbezpieczeństwa.

**Stan obecny**

Zamawiający zarządza obecnie urządzeniami, które łączą się na pośrednictwem sieci LAN w trzech lokalizacjach tj. szpital w Poznaniu, szpital w Ludwikowie, szpital w Chodzieży. W ramach zapewnienia bezpiecznej transmisji wykorzystywany jest VPN do głównego ośrodka mieszczącego się w szpitalu w Poznaniu.

**Zamawiający w ramach przedmiotu zamówienia wymaga :**

Dostarczenie urządzeń, licencji oraz wdrożenie, konfiguracja urządzeń i oprogramowania w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych w zakresie cyberbezpieczeństwa. W szczególności:

# Zintegrowany System bezpieczeństwa dla lokalizacji szpital Poznań szt. 1

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.

W szczególności:

## Redundancja, monitoring i wykrywanie awarii

1. 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.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

## Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
* 16 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
* 2 gniazdami SFP+ 10 Gbps.
1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

## Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

## Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zapora ogniowa klasy StatefulInspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - IntrusionPrevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Trafficshaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

## Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. 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.
1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. 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

1. 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/CounterMode(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-sharedkey, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSecsite-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.
1. 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.
* Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

## Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equalcostmulti-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (BidirectionalForwardingDetection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

## Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

## Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

## Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. 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.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. 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.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

## Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

## Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. 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

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. 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.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja SafeSearch – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

## Uwierzytelnianie użytkowników w ramach sesji

1. 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.
1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. 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.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

## Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

## Logowanie

1. 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.
2. 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.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

## Certyfikaty

Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.

## Testy wydajnościowe oraz funkcjonalne

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

## Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandboxcloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

## Gwarancja oraz wsparcie

Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

## Rozszerzone wsparcie serwisowe AHB/SOS

System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy.

System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta świadczonym w języku polskim przez okres 12 miesięcy w zakresie:

* Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
* Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
* Doradztwo w zakresie konfiguracji.
* Zdalne wsparcie techniczne.
* Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
* Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
* Przygotowanie urządzenia do zdalnej konfiguracji.
* Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
* Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
* Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
* Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

Wymagania powinny być potwierdzone dokumentami:

* Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
* Certyfikat ISO 9001 podmiotu serwisującego.

# Zintegrowany System bezpieczeństwa dla pozostałych lokalizacji szt. 2

Wszystkie opisy zawarte w pkt 1 za wyjątkiem pkt 1.2, który przyjmuje brzmienie pkt2.1 oraz pkt 1.3, który przyjmuje brzmienie pkt 2.2:

## Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
* 10 portami Gigabit Ethernet RJ-45.
1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

## Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

# Zintegrowany System bezpieczeństwa –centralny system logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji.Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na systemielinux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXiwerje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; CitrixXenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

## Interfejsy, Dysk:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności minimum 10 TB.

## Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

## Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
* Listę najczęściej wykrywanych ataków.
* Listę najbardziej aktywnych użytkowników.
* Listę najczęściej wykorzystywanych aplikacji.
* Listę najczęściej odwiedzanych stron www.
* Listę krajów , do których nawiązywane są połączenia.
* Listę najczęściej wykorzystywanych polityk Firewall.
* Informacje o realizowanych połączeniach IPSec.
1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
2. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
3. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

## Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

## Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
* Malware.
* Aplikacje sieciowe.
* Email.
* IPS.
* Traffic.
* Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
1. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.

## Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

1. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

## Serwisy i licencje

1. System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

# System kontroli dostępu do zasobów sieciowych - NAC

## Podstawowe funkcjonalności systemu NAC

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami sieciowymi wielu producentów (tzw. multivendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 1500 jednoczesnych unikatowych urządzeń końcowych /adresów MAC/ do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 50000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (BringYourOwn Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
* VM – min. VMWareESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, CitrixXenServer w wersji min 4.x
* Maszyny fizyczne - serwery wspierane przez producenta.
1. System musi posiadać funkcjonalność serwerów:
* serwera RADIUS dla infrastruktury sieciowej,
* serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
* serwera VPN,
* serwera DNS,
* serwera SYSLOG,
* serwera TFTP,
* serwera TACACS+,
* serwera Monitoringu,
* serwera DHCP,
* serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
* serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
1. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.
2. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
3. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.
4. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z innych systemów zewnętrznych.
5. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, konfiguracji VPN, wysłania konfiguracji dostępowych poprzez email.
6. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
7. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
8. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.
9. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
10. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
11. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. tożsamość, MAC adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
12. System musi zapewniać scentralizowane zarządzanie urządzeniami sieciowymi. Zarządzanie musi odbywać się bezagentowo, a w systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
13. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
14. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych i końcowych za pomocą min. protokołu SNMP.
15. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu: VLANów, autoryzacji, statusu, opisu.
16. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
17. System musi zapewniać funkcjonalność wizualizacji konfiguracji podsieci IP oraz przypisania jej do jednostek.
18. System musi posiadać funkcję zintegrowanego serwera DHCP.
19. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
20. System musi wspierać funkcjonalność włączania i wyłączania podsieci IP, adresów IP bez konieczności usuwania ich z systemu.
21. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
22. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP.
23. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
24. System musi posiadać wbudowany Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
25. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS.
26. Portal musi umożliwiać obsługę instalacji agentów, dystrybucji certyfikatów użytkowników oraz generowania autokonfiguratorów sieci.
27. System musi posiadać mechanizm zarządzania uprawnieniami użytkowników, którzy będą mogli rejestrować swoje urządzenia, pobierać certyfikaty, agenty oraz uruchamiać autokonfiguratorów sieci.
28. Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
29. Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
30. Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
31. Interfejs graficzny Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
32. Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
33. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
34. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
35. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
36. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
37. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
38. System musi obsługiwać metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej:
* DHCP Fingerprinting
* DHCP SPAN
* SNMP
* Vendor OUI
* TCP
* Active Directory
* CDP/LLDP
* HTTP/S
* DNS
* Radius
* WMI
* MDM
* WinRM
* ONVIF
1. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach:
* FortiGate
* PulseSecure
* OpenVPN
* PaloAlto
* Cisco ASA
1. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa.
2. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Portal.
3. System musi współpracować z serwerem tokenów.
4. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:
* Microsoft Windows
* Mac OS
* iOS
* Android
1. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).
2. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
3. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
* wiadomości e-mail,
* Syslog,
* notyfikacji systemowych.
1. System musi zapewniać wsparcie dla obsługi serwerów TACACS+.

## Mechanizmy uwierzytelniania

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
* MAC,
* PAP/ASCII,
* CHAP,
* SNMP,
* 802.1X.
1. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), itp.
2. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
3. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
4. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Apple Mac OS X Supplicant, Apple iOSSupplicant, Google Android Supplicant, UbuntuSupplicant).
5. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
* Tożsamość/Urządzenie końcowe,
* Grupa tożsamości/urządzeń końcowych,
* Parametry urządzeń końcowych, min: system operacyjny, wersja,
* Atrybuty Active Directory,
* Jednostka organizacyjna tożsamości/urządzeń końcowych,
* Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
* Grupy urządzeń sieciowych,
* Porty urządzeń sieciowych,
* Grupy portów urządzeń sieciowych,
* Jednostka organizacyjna portów,
* Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
* Data, czas ważności polityki,
* Wewnętrzny Captive Portal,
* Metoda autoryzacji.
1. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
2. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
3. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
4. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
5. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
6. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
7. System musi pozwalać na weryfikację zalogowanego urządzenia końcowego IoT (Internet of Things) minimum za pomocą mechanizmów SNMP, DHCP, NMAP, Agenta oraz wywołania akcji: powiadomienie administratorów i/lub zablokowanie i rozłączenie sesji.
8. System musi wspierać funkcjonalność różnych typu autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
9. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
10. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

## Obsługa serwerów certyfikatów CA

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
* możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
* możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
* Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple CertificateEnrollmentProtocol).
* usługę OCSP (Online Certificate Status Protocol).

## Obsługa serwerów VPN

1. System musi posiadać funkcję zintegrowanego serwera VPN oraz zapewniać współpracę z zintegrowanym oraz zewnętrznym serwerem CA,
2. System musi umożliwiać wystawianie konfiguracji klienckich, certyfikatów dla serwerów VPN.
3. System musi logować wszelkie próby autoryzacji do serwerów VPN.
4. System musi zapewniać przynajmniej następujące funkcjonalności serwera VPN:
* Logowanie do zasobów firmy,
* Obsługę OTP,
* Przypisanie ustalonego adresu IP.

## Obsługa serwerów DNS

1. System musi posiadać funkcję zintegrowanego serwera DNS.
2. System musi umożliwiać graficzne zarządzanie serwerami DNS.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DNS:
* Zarządzanie strefami,
* Zarządzanie rekordami stref,
* Zatwierdzanie przez administratorów moderowanych rekordów stref,
* Weryfikacja konfiguracji przed instalacją,
* Instalacja konfiguracji na serwerach DNS.

## Obsługa serwerów DHCP

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
* Uruchamianie usługi dla wybranych podsieci,
* Przypisanie ustalonego adresu IP dla adresu MAC.
* Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
* Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
* Możliwość określania braku dostępu dla wybranych adresów MAC,
* Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
* Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
* Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
* Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
* Dokonywanie zmian bez konieczności wyłączania usług.

## Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.

## Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring zdarzeń autoryzacji
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadam adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory.

## Alarmy

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą wiadomości e-mail, Syslog, notyfikacji systemowych.
2. Alarmy mogą być generowane w sytuacjach, min: Ilości obsługiwanych transakcji RADIUS, opóźnienie obsługi transkacji RADIUS, statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
* badanie łączności IP za pomocą ping, traceroute,
* tcpdump protokołów RADIUS, TACACS+,
* wyszukiwanie zdarzeń RADIUS z uwzględnieniem nazwy użytkownika, adresu MAC, statusu uwierzytelnienia (udana lub nieudana), powodu, jeżeli uwierzytelnienie nieudane, zakresu czasowego, co do dnia, godziny i minuty, wykonanie zdalnego polecenia na urządzeniu sieciowym.

## Dostawa, wdrożenie, wsparcie techniczne i szkolenie

1. System musi zostać dostarczony z licencją dożywotnią oraz wsparciem technicznym zapewniającym przez okres minimum 3 lat dostępu do aktualizacji oferowanego oprogramowania do najnowszej wersji udostępnianej przez producenta.
2. Wsparcie techniczne powinno dodatkowo gwarantować:
* Możliwość kontaktu z działem wsparcia technicznego producenta w języku polskim za pomocą poczty elektronicznej.
* Pomoc przy identyfikacji i rozwiązywaniu problemów związanych z oprogramowaniem.
* Dostęp poprzez stronę internetową do dokumentacji technicznej, aktualizowanej wraz z pojawianiem się nowych wersji oprogramowania.
* Dostęp do aktualizacji oraz poprawek oprogramowania z poziomu interfejsu oprogramowania przez cały okres obowiązywania wsparcia technicznego.
1. Zamawiający wymaga uruchomienia i wdrożenia systemu w środowisku sieciowym Zamawiającego oraz wykonanie dokumentacji. Prace wdrożeniowe muszą obejmować w szczególności następujące elementy:
* Dostawa, instalacja, konfiguracja wstępna i licencjonowanie produktu w środowisku wirtualizacyjnym Zmawiającego.
* Firewall - dostosowanie komunikacji podsieci przełączników z podsiecią systemu NAC.
* Podstawowa konfiguracja (integracja z domeną, definicja obiektów podsieci, definicja obiektów VLAN, MAC na podstawie dostarczonych przez Zamawiającego list).
* Integracja z przełącznikami i kontrolerami WiFi, obszarowe wdrażanie autoryzacji (uruchamianie na portach, testy).
* Wdrażanie autoryzacji na przełącznikach - obejmuje uruchomienie autoryzacji na wszystkich możliwych portach dostępowych (min. 100 szt. przełączników), testy poprawności autoryzacji.
* Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list adresów MAC).
* Konfiguracja polityk uwierzytelniania w systemie w oparciu o certyfikaty i/lub poświadczenia AD oraz MAC, testy i optymalizacja.
* Konfiguracja GPO w ramach funkcjonującego AD, uruchamiającego suplikanta dla sieci przewodowej i bezprzewodowej, testy.
* Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń.
1. Szkolenie podstawowe z obsługi systemu (sesja online) dla minimum 7 osób.

# System zabezpieczenia danych przed wyciekiem - DLP

System zapewniający kontrolę m.in. nad urządzeniami peryferyjnymi, w tym szczególnie urządzeniami podłączanymi poprzez porty USB oraz kontrolę poufnych danych wysyłanych poza sieć firmową, oferując równocześnie funkcjonalności szczegółowego raportowania rejestrowanych zdarzeń

## Parametry techniczno-funkcjonalne

1. System musi wykrywać zagrożenia związane z utratą, wyciekiem lub kradzieżą danych generowanych przez kontrolowane urządzenia, przenośne pamięci masowe, porty peryferyjne. Rozwiązanie musi zapewniać ochronę danych będących w ruchu, filtrować poufne dane organizacji, które mogą być przesyłane poza sieć wewnętrzną poprzez różne punkty wyjścia, takie jak: przeglądarki, emaile, usługi chmurowe, media społecznościowe.
2. System musi umożliwiać administratorom IT zarządzanie wszystkimi komputerami w sieci (Windows, Mac OS X i Linux) ze scentralizowanej, webowej konsoli zarządzania. Lokalny agent musi być zainstalowany na każdym chronionym komputerze.
3. System musi mieć architekturę klient-serwer i być dostępnym w trzech wariantach:
* Urządzenie wirtualne (virtualappliance) minimum w formatach:
Vmware Workstation, Vmware Player, VmwarevSphere (ESXi), VmwareFusion, OracleVirtualBox, Parallels Desktop Mac. Microsoft Hyper-V Server 2008-2012, CitrixXenServer (formaty plików maszyn wirtualnych: .VMX, .OVF, .OVA, .XVA, .VHD, .PVM), wstępnie skonfigurowanych przez producenta,
* Urządzenie sprzętowe (hardware appliance), w formie gotowego sprzętu z dedykowanymi licencjami i akcesoriami, który można zamontować w szafie rack (19 cali).
* Obraz wirtualny, dostosowany do implementacji w środowisku chmurowym (azure, googlecloud, amazon).
1. Klient musi być dostępny minimum dla następujących rodzin systemów operacyjnych: Windows, Mac OS X, Linux. Szczegółowy wykaz minimalnych wymagań w zakresie wspieranych wersji systemów operacyjnych:
* Windows (32/64 bitowy): Windows 11, Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2008, Windows 2003,
* Mac: Mac OS 12.0, Mac OS 11.0, Mac OS 10.15, Mac OS 10.14, Mac OS 10.13, Mac OS 10.12, Mac OS X 10.11, Mac OS X 10.10, Mac OS X 10.9, Mac OS X 10.8, Mac OS X 10.7
* Linux: Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, OpenSUSE/SUSE 12.1 – 12.4, CentOS/RedHat 7.0+, CentOS/RedHat 6.0+, Fedora 27 oraz 29, Debian 9.8, Mint 18.x, Oracle 7.4+
1. Komunikacja między serwerem a klientem musi odbywać się za pośrednictwem bezpiecznego połączenia (https) na dowolnie konfigurowanym porcie.
2. Rozwiązanie musi zapewniać integrację z Active Directory (AD), co oznacza, że ​​elementy składowe AD (w tym szczególnie: jednostki organizacyjne, grupy, komputery, użytkownicy) mogą być importowane na serwer systemu DLP. Dodatkowo wymagana jest możliwość włączenia mechanizmu synchronizacji zmian z AD. Instalacja agenta na wszystkich komputerach w sieci musi być możliwa w sposób zautomatyzowany, bez angażowania użytkownika stacji końcowych.
3. Rozwiązanie musi zapewniać dostęp do systemu DLP zarówno z sieci wewnętrznej lub zewnętrznej. Administrator musi mieć możliwość połączenia się za pomocą nazwy użytkownika i hasła z dowolnego komputera w sieci wewnętrznej lub przez Internet, jeśli rozwiązanie zostanie wdrożone w wariancie z zewnętrznym adresem IP.
4. Interfejs zarządzający rozwiązania musi być dostępny minimum w języku polskim i angielskim.
5. Producent musi oferować możliwość rocznego, dwuletniego oraz trzyletniego przedłużenia licencji zawierającej wsparcie techniczne oraz aktualizacje rozwiązania.
6. Rozwiązanie musi posiadać co najmniej dwa poziomy uprawnień dla kont administratorów:
* konto administratora (root) z pełnymi uprawnieniami do zarządzania systemem DLP,
* konta administratorów z ograniczonymi uprawnieniami.
1. System musi mieć możliwość nadawania odpowiednich ról dla administratorów, które ograniczą ich możliwości zarządzania systemem,
2. Rozwiązanie musi pozwalać na utworzenie oddzielnych zestawów konfiguracji polityk bezpieczeństwa, dedykowanych jednostkom organizacyjnym danej firmy, łącznie z możliwością utworzenia konta administratora delegowanego do zarządzania danym modułem.
3. Administrator systemu DLP musi mieć możliwość zdefiniowania minimum następujących akcji dla przenośnych pamięci masowych używanych wewnątrz organizacji:
* blokuj,
* zezwól,
* tylko do odczytu.
* pozwól gdy urządzenie jest szyfrowane (dostęp tylko do części szyfrowanej)
1. Uprawnienia muszą być przydzielane co najmniej na następujących poziomach:
* globalnie (ustawienia mają zastosowanie do wszystkich komputerów chronionych systemem DLP),
* poziom grupy (ustawienia odnoszą się do komputerów i użytkowników w grupie),
* poziom komputera (ważny dla jednego komputera),
* poziom użytkownika (ustawienia dostępne dla pojedynczego użytkownika),
* poziom urządzenia (ustawienia dostępne dla określonego urządzenia przenośnego).

Administrator musi mieć możliwość zmiany priorytetu ustawień dla poziomu komputera lub użytkownika.

1. System musi identyfikować i zarządzać co najmniej wymienionymi poniżej urządzeniami oraz portami peryferyjnymi, z następującymi prawami:
* urządzenia pamięci USB - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu / Zezwalaj na dostęp, jeśli urządzenie jest zaufane / Zezwalaj na dostęp, jeśli urządzenie jest zaufane a jeśli nie jest zaufane – tylko do odczytu
* wewnętrzny napęd CD/ DVD RW - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
* wewnętrzny czytnik kart pamięci - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
* wewnętrzny napęd dyskietek - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
* drukarki lokalne - Odmów dostępu / Zezwalaj na dostęp,
* przenośne urządzenia z systemem Windows - Odmów dostępu / Zezwalaj na dostęp
* aparat cyfrowy - Odmów dostępu / Zezwalaj na dostęp,
* BlackBerry - Odmów dostępu / Zezwalaj na dostęp,
* SmartPhone (Windows CE) - Odmów dostępu / Zezwalaj na dostęp,
* SmartPhone (Symbian) - Odmów dostępu / Zezwalaj na dostęp,
* Android Smartphone (Media Transfer Protocol) - Odmów dostępu / Zezwalaj na dostęp,
* iPhone - Odmów dostępu / Zezwalaj na dostęp,
* iPad - Odmów dostępu / Zezwalaj na dostęp,
* iPod - Odmów dostępu / Zezwalaj na dostęp,
* kamera internetowa - Odmów dostępu / Zezwalaj na dostęp,
* kontroler Serial ATA - Odmów dostępu / Zezwalaj na dostęp,
* WiFi - Odmów dostępu / Zezwalaj na dostęp / Blokuj Wi-Fi, jeśli jest dostępna sieć przewodowa,
* Bluetooth - Odmów dostępu / Zezwalaj na dostęp,
* FireWire - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
* port szeregowy - Odmów dostępu / Zezwalaj na dostęp,
* port równoległy (LPT) - Odmów dostępu / Zezwalaj na dostęp,
* PCMCIA - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
* MTD - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
* SCSI - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
* napęd ZIP - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
* Thunderbolt - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
* udziały sieciowe - Odmów dostępu / Zezwalaj na dostęp,
* port podczerwieni - Odmów dostępu / Zezwalaj na dostęp,
* Thin Client Storage (RDP Storage) - Odmów dostępu / Zezwalaj na dostęp / Tylko do odczytu,
* dodatkowa klawiatura - Odmów dostępu / Zezwalaj na dostęp,
* modem USB - Odmów dostępu / Zezwalaj na dostęp / blokuj w przypadku obecności sieci przewodowej,
* Nieznane urządzenie - Odmów dostępu / Zezwalaj na dostęp.
1. Administrator musi mieć możliwość monitorowania, które pliki zostały skopiowane przez użytkowników (pracowników) i na jakie urządzenia. System musi pozwalać na generowanie raportów obejmujących co najmniej następujące informacje:
* jaki plik został przesłany / usunięty / z edytowany
* typ i rozmiar,
* użytkownik,
* nazwa komputera i adres IP z którego dokonano transferu,
* nazwa urządzenia przenośnego wraz z numerem seryjnym (jeśli dostępny),
* data i godzina przekazania, funkcje skrótu pliku.
1. System musi pozwalać na eksportowanie raportów jako pliki CSV, PDF, Excel do lokalizacji określonej przez administratora.
2. Administrator musi mieć możliwość włączenia lub wyłączenia powiadomień dla użytkowników o zablokowanych akcjach na stacjach roboczych
3. Administrator musi mieć możliwość ustalenia godzin w jakich będą obowiązywały polityki firmowe.
4. Administrator musi mieć możliwość ustalenia sieci LAN w jakich będą obowiązywały polityki firmowe.
5. Administrator musi mieć możliwość ustalenia limitu wielkości lub ilości przesyłanych plików w danej jednostce czasu.
6. Rozwiązanie musi pozwalać administratorowi na kontrolowanie przesyłania plików za pośrednictwem minimum następujących aplikacji internetowych:
* przeglądarki internetowe: Internet Explorer, Chrome, Mozilla Firefox, Opera, Safari, AOL Desktop 9.6, Aurora Firefox, Brave, Adobe Flash Player, Tor, Camino, iCab, OmniWeb, Sleipnir, K-Meleon, SeaMonkey, Maxthon, FrontMotionFirefox, Pale Moon, Swing, Torch, Whale
* klienci pocztowi: Outlook, Outlook (Body), Mozilla Thunderbird, Mozilla Thunderbird (Body), IBM Lotus Notes v.6.5-v.9.0, IBM Lotus Notes v.6.5-v.9.0 (Body), Geary, Evolution, Claws Mail, Sylpheed, Balsa Mail Client, Windows Live Mail, GroupWise Client, Foxmail, SeaMonkey Mail, Zimbra Desktop Mail, Eudora, eM Client, Sparrow, GyazMail, PowerMail, AirMail Beta, Sparrow Lite, Postbox, Mail, Outlook Express, Windows Mail, AOL Mail, Courier, Opera Mail,
* Komunikatory internetowe: ICQ, AIM, Skype, Windows Live Messenger, Yahoo Messenger, Gaim, Pidgin, Trillian, NateOn Messenger, Spark, Telegram Desktop, Messages, Audium, Line, Hall, OpenTalk, TurnoIRC, WinSent Messenger, xChat, TweetDeck, Pink Notes Plus, Google Talk, Thwirl, QQ International, mIRC, MySpace IM, DuamMyPeople, Kakao Talk, Chit Chat for Facebook, eBuddy, Facebook Messenger, fTalk, Microsoft Communicator 2007, LingoWare, Lan Chat Enterprise, My Chat, Nimbuzz, ooVoo, Microsoft Link, Mail.Ru Agent, Slack, Psi+, Viber, Discord, Zalo, WhatsApp Desktop
* Usługi chmurowe / Udostępnianie plików: Google Drive Client, iCloud Client, uTorrent, BitComet, Daum Cloud, KtOllehuCloud, Azureus, Box Sync, Sugar Sync, Picasa, Amazon Drive, iBooks Author, MediaFire Client, Novell Filr Client, AirDrop, Transmission, Morpheus, FileCloud Sync Client, OneDrive (Skydrive) Client, Lime Wire, FTP Command, BitTorrent, ownCLoud Client, Pogoplug Backup, Shareaza, Pruna P2P, SendSpace, DC ++, Dropbox, eMule, Evernote, Kazaa, Android File Transfer, GitHub Client, MEGA, Yandex Desk, KRDC, qBittorrent, Linex DC++, Webhard, Send Anywhere, SideSync
* Media społecznościowe / Inne: Windows Apps, EasyLock, Team Viewer, Windows DVD Maker, Total Commander, ALFTP, LogMeIn Pro, iTunes, FileZilla, SCP, total Commander 64 bit, Sony Ericsson PC Companion, InfraRecorder CD-DVD, HTC Sync for Android, GoToMeeting, Nokia PC Suite 2011 Video Transfer, Nokia PC Suite 2011 Image Store, Nokia PC Suite 2011, Nokia PC Suite 2008 Main, Nokia PC Suite 2008, Zoom, Station, VNC, Wormhole Switch DSS, Samsung DeX, Samsung Kies, PowerShell, iMazing, CuteFTP,
1. Rozwiązanie musi pozwalać administratorom na kontrolowanie przesyłania plików za pomocą funkcjonalności filtrów działających minimum w oparciu o:
* typ pliku,
* wykryty kod źródłowy,
* wstępnie zdefiniowaną zawartość,
* spersonalizowaną treść,
* nazwę pliku,
* wyrażenia regularne.
1. Filtry bazujące na rozszerzeniach plików muszą pozwalać na wykrywanie minimum poniższych rodzajów plików:
* pliki graficzne: JPEG, PNG, GIF, ICO, BMP, TIFF, CGM, Corel Photo – Paint, CorelDraw, DJV, EPS, Adobe Illustrator, Adobe inDesign, BPF, PSD,
* pliki pakietu Microsoft Office: Word, Excel, PowerPoint, PDF, Infopath, Outlook, Publisher, iWork files, Office 2007+/password,
* archiwa plików: ZIP, ZIP/password, 7z, RAR, ACE, TAR, XZ, .XAR, ACE/password, RAR/password, BZ2, GZ,
* pliki multimedialne: Mov, Mp3, M4a, mp4, Wav, Wma, Avi, Aif, M3u,
* pozostałe pliki: Textfiles, DRM Files, Exe, sys, dll, FasooFiles, Journalfiles, so, unindetified, .accdb, Bdf, Csr, DTA, EPP\_ENCRYPTED FILES, FDL, NASCA DRM, P12, SgWgc, SID, SSD, VMDK, Xia, XML / DTD, FDL, HUE, RODE, SEGD, SEGY,
* CAD files: AutoCAD, I-DEAS 3D CAD, IGS, Pro-E CAD, Prt, REVIT, SMG, SOLID EDGE, SolidWorks, STL, WRL, XDL, CATIA,

Na życzenie użytkownika systemu DLP producent rozwiązania powinien dodać niezbędne, brakujące typy plików.

1. System musi posiadać możliwość kontroli wysyłki kodu źródłowego, wraz z zaimplementowanym mechanizmem uczenia maszynowego, który pozwala na zmniejszenie ilości false-positivów wraz z tokiem nauki,
2. System musi posiadać predefiniowane polityki, które będą zgodne co najmniej z regulacjami:
* HIPAA
* PCI
* GDPR / RODO
1. System musi posiadać możliwość blokowania dostępu do wybranych domen i/ lub adresów URL
2. System musi posiadać możliwość zezwolenia na dostęp i wysyłania plików do wybranych domen i/lub adresów URL
3. System musi posiadać sprawdzanie danych aplikacji na niestandardowych portach, zdefiniowanych przez administratora.
4. System DLP musi pozwalać na zdefiniowanie co najmniej trzech akcji związanej z zadziałaniem polityki kontrolowania plików:
* tylko raportuj,
* tylko blokuj,
* blokuj i raportuj,
1. Predefiniowane filtry zawartości muszą umożliwiać administratorom zautomatyzowane zarządzanie transferem plików zawierających dane wrażliwe, rozumiane jako co najmniej:
* numery kart kredytowych,
* numery IBAN,
* numery SWIFT,
* numery PESEL,
* adresy korespondencyjne,
* adresy e-mail,
* numery telefonów,
* numery dowodów osobistych
* numery NIP
* Adresy protokołów internetowych w wersji 4 i 6
1. System musi umożliwiać tworzenie niestandardowych filtrów treści dających administratorom możliwość zarządzania transferem plików na podstawie słów kluczowych.
2. System musi umożliwiać zarządzanie transferem plików zawierających dane rekurencyjne, na podstawie definiowalnych przez administratora filtrów korzystających z wyrażeń regularnych.
3. W przypadku wykrycia kopiowania pliku z wrażliwymi danymi rozwiązanie musi pozwalać na utworzenia jego duplikatu na serwerze systemu DLP (tzw. funkcjonalność „File Shadow”).
4. Rozwiązanie musi posiadać także funkcjonalność śledzenia i zachowywania informacji o ruchu wszystkich plików przenoszonych przez dowolnego użytkownika podłączonego do chronionego komputera.
5. System musi posiadać zintegrowany moduł automatycznego szyfrowania plików przenoszonych na urządzenia przenośne.
6. Rozwiązanie musi mieć możliwość wysyłania w czasie rzeczywistym alertów przez e-mail do administratorów, gdy wykryte zostanie predefiniowane zdarzenie (np. możliwy wyciek danych).
7. System musi posiadać możliwość tworzenia własnych okien, aby powiadamiać użytkownika o wykonywanej akcji.
8. Rozwiązanie musi być w stanie dostarczyć statystyki i wykresy dotyczące korzystania z urządzeń przenośnych i transferu plików w sieci.
9. Rozwiązanie musi zapewniać ciągłą ochronę komputera, nawet jeśli jest odłączony lub usunięty z sieci wewnętrznej. Ustawienia polityk ochrony muszą pozostać aktywne, nawet jeśli komputer nie ma połączenia z serwerem systemu DLP. Wygenerowane w tym czasie logi i raporty muszą być przechowywane lokalnie na danym komputerze a przy ponownym połączeniu z serwerem muszą zostać do niego przesłane.
10. Oprogramowanie agentów systemu DLP na stacjach końcowych musi być chroniony hasłem zapobiegającym odinstalowaniu agenta.
11. Rozwiązanie musi pozwalać administratorowi na czasowe autoryzowanie podłączenia pamięci USB do komputerów, nawet gdy komputer nie jest podłączony do serwera systemu DLP.
12. Rozwiązanie musi pozwalać administratorowi na wymuszenie podania powodu użycia czasowej autoryzacji w celu podłączenia pamięci USB do komputerów.
13. System musi pozwalać administratorom dostosować interwał komunikacji między agentami a serwerem (czas w którym klient wysyła logi i raporty do serwera).
14. System musi pozwalać administratorom zdefiniować "białą listę" plików, które można kopiować na autoryzowane urządzenia.
15. System musi pozwalać administratorom na zdefiniowanie "białej listy" adresów URL i domen, do których możliwe będzie przesyłanie plików.
16. Rozwiązanie musi posiadać funkcjonalność aktualizacji, umożliwiającą instalowanie najnowszych dostępnych wersji z poziomu webowej konsoli zarządzającej.
17. Webowa konsola zarządzająca musi pozwalać na:
* zdefiniowanie, zmianę oraz kontrolę bieżących ustawień systemu DLP,
* dostęp do raportów i danych statystycznych związanych z działaniem systemu DLP,
* wyłączenie oraz restart systemu DLP.
1. Rozwiązanie musi pozwalać administratorom na wysyłanie wiadomości bezpośrednio do działu pomocy technicznej producenta. Wsparcie techniczne musi być oferowane co najmniej w języku angielskim.
2. System musi obsługiwać optyczne rozpoznawanie znaków (OCR).
3. System DLP musi pozwalać na integrację z zewnętrznymi rozwiązaniami SIEM, rozumianą jako możliwość przesyłania rejestrowanych zdarzeń do zewnętrznego serwera SIEM w celu ich analizy i raportowania.
4. System DLP musi mieć możliwość blokowania dostępu na dane strony internetowe, zdefiniowane przez administratora.
5. System DLP opcjonalnie musi pozwalać administratorowi na tworzenie polityki aktywnego sprawdzania/skanowania danych znajdujących się na chronionych komputerach Mac, Windows i Linux, umożliwiając egzekwowanie wewnętrznej polityki bezpieczeństwa danych firmy oraz zarządzanie ryzykiem stwarzanym przez przypadkowe lub zamierzone wycieki danych. Rozwiązanie musi umożliwiać co najmniej dwa rodzaje skanów:
* skan początkowy (czysty): wykrywanie danych wrażliwych od zera,
* skan przyrostowy: kontynuacja wykrywania (pomijając wcześniej zeskanowane pliki).

Administrator musi mieć możliwość zarządzania wynikami skanowania, w tym listą wszystkich komputerów, które były skanowane. Rozwiązanie (w zakresie funkcjonalności aktywnego skanowania) musi pozwalać na podjęcie minimum następujących akcji:

* usuwanie,
* szyfrowanie lub odszyfrowywanie plików.

Administrator musi mieć możliwość zastosowania żądanej akcji do każdego elementu indywidualnie lub do grupy wybranych elementów jednocześnie.

1. System DLP musi opcjonalnie posiadać moduł szyfrowania podłączanych pamięci USB

## Dostawa, wdrożenie, wsparcie techniczne i szkolenie

1. Wymagane jest aby producent zapewniał wsparcie techniczne minimum przez: telefon, e-mail, czat na żywo oraz zdalne połączenie przez okres minimum 3-ech lat
2. Minimalna liczba licencji to 501 sztuk
3. Instalacja oprogramowania na wskazanym serwerze.
4. Logiczne podłączenie interfejsów sieciowych.
5. Aktywacja maszyny wirtualnej oraz wstępna konfiguracja:
* aktywacja licencji,
* konfiguracja ustawień oraz preferencji systemowych i sieciowych,
* integracja systemu z usługami katalogowymi AD.
1. Konfiguracja polityk bezpieczeństwa:
* konfiguracja ustawień agentów, między innymitryb pracy agentów oraz częstotliwość aktualizacji polityk,
* dodanie zaufanych urządzeń do systemu,
* ustawienie praw urządzeń dla poszczególnych grup
* przygotowanie czarnych oraz białych list,
* konfiguracja polityk kontroli wysyłanej treści poprzez aplikacje desktopowe,
1. Konfiguracja kopii zapasowych.
2. Przygotowanie paczek instalacyjnych agentów.
3. Wykonawca przeprowadzi szkolenie administracyjne dla minimum 5 osób

# System wykrywania incydentów i działań naprawczych - EDR

## Parametry techniczno-funkcjonalne

1. Pełna ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami
2. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi
3. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog2
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
5. Wbudowaną technologię do ochrony przed rootkitami.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. Możliwość skanowania dysków sieciowych i dysków przenośnych.
10. Skanowanie plików spakowanych i skompresowanych.
11. Możliwość dodawania wykluczenia na podstawie
* Plik
* Folder
* Rozszerzenie
* Proces
* Hash pliku
* Hash certyfikatu
* Nazwa zagrożenia
* Wiersz poleceń
* IP/maska
1. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.
2. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
3. Automatyczną integrację skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
4. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
5. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
6. Automatyczną integrację z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
7. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
8. Możliwość skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.
9. Możliwość skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
10. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program będzie pytał o hasło.
11. Możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony.
12. Możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
13. Możliwość wyświetlenia kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia.
14. Automatyczną, inkrementacyjną aktualizację baz wirusów i innych zagrożeń.
15. Obsługę pobierania aktualizacji za pośrednictwem serwera proxy.
16. Praca programu musi być niezauważalna dla użytkownika.
17. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.
18. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
19. posiadać wbudowaną funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
20. Możliwość odblokowania ustawień programu po wpisaniu hasła
21. Możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu
22. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie)
23. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu.
24. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.
25. Funkcja Ochrony danych konfigurowana zdalnie przez administratora.
26. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.
27. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
28. Wbudowany IDS
29. Możliwość zainstalowania silnika pełnego, lekkiego ze sprawdzaniem reputacji plików w chmurze, lub wykorzystanie dodatkowej maszyny wirtualnej która przejmie rolę silnika skanującego.
30. Maszyna która przejmuję rolę silnika skanującego musi działać w trybach redundancji lub równej dystrybucji
31. Aktualizacja maszyny skanującej musi obejmować oddzielną aktualizację nowych funkcji, ulepszeń, poprawek oraz oddzielną aktualizację systemu operacyjnego urządzenia wirtualnego.
32. Możliwość tworzenia list sieci zaufanych.
33. Możliwość dezaktywacji funkcji zapory sieciowej.
34. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
35. Funkcję ochrony przeciwko znanym zagrożeniom typu ransomware
36. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji
37. Możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań(konfigurowalne w politykach bezpieczeństwa)
38. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy securitygroups
39. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.
40. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:
* Możliwość wymuszenia funkcji DEP systemu Windows
* Możliwość wymuszenia relokacji modułów (ASLR)
1. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochroną przed technikami takimi jak:
* -Wczesny dostęp
* -Dostęp do poświadczeń
* -Wykrycie
* -Crimeware
1. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji.
2. Ochrona proaktywna oparta o maszynowe uczenie która działa w fazie poprzedzającej wykonanie, ochrona ta musi wy wykrywać zagrożenia takie jak:
* Ukierunkowane ataki
* Podejrzane pliki i ruch w sieci
* Exploity
* Ransomware
* Grayware
1. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego
2. Moduł ochrony proaktywnej musi działać w trybach które administrator może dowolnie zmieniać na:
* Tolerancyjny
* Normalny
* Agresywny
1. Zintegrowany sandbox po stronie producenta który pozwala na analizę pliku
* Plik może zostać wysłany automatycznie ze stacji roboczej jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora
* Możliwość przesłania archiwum zabezpieczonego hasłem
* Możliwość przesłania adresu URL
* W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.
1. Wbudowany sandbox musi działać w trybie monitorowania i blokowania
2. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny
3. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania.
4. Wbudowany sandbox musi posiadać opcję która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.
5. Minimalny rozmiar pliku jaki może zostać przesłany do sandboxa to 1KB
6. Maksymalny rozmiar pliku jaki może zostać przesłany do sandboxa to 50MB
7. Telemetria1 - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM Splunk(wymaga TLS 1.2 lub wyższy)
8. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników zagrożeń, wskaźniki te obejmują:

## Maszyny Wirtualne

1. Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu)
2. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
3. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem
4. Wersja kliencka nie pełni roli ochrony antywirusowej, jest tylko agentem dla Security Servera.
5. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
6. Możliwość określenia co jaki czas mają być wysyłane pliki z kwarantanny do producenta.
7. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
8. Możliwość wskazania do jakiego serwera ochrony maja się łączyć klienci maszyn wirtualnych.

## Stacje robocze i serwery typu Windows

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
4. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
5. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
6. Skanowanie plików spakowanych i skompresowanych.
7. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
8. Oprogramowanie posiada możliwość zablokowania hasłem odinstalowania programu.
9. Produkt oraz sygnatury muszą być aktualizowane nie rzadziej niż raz na godzinę.
10. Oprogramowanie musi posiadać możliwość raportowania zdarzeń informacyjnych.
11. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
12. Program musi posiadać możliwość skanowania jedynie nowych nie zmienionych plików.
13. Program musi mieć wbudowany skaner wyszukiwania rootkitów
14. Możliwość odblokowania ustawień programu po wpisaniu hasła
15. Możliwość uruchomienia zadania skanowania z niskim priorytetem
16. Możliwość wykorzystania dodatkowej maszyny wirtualnej która przejmie role silnika skanującego.
17. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
18. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem
19. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
20. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.

## Ochrona Exchange

1. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.
2. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w przeciągu ostatnich kilku godzin / dni.
3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz nie możliwych do przeskanowania.
4. Możliwość wykluczenia potencjalnie niechcianych aplikacji (PUA) z filtrowania antymalware.
5. Możliwość skanowania w poszukiwania malware wewnątrz archiwów.
6. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen.
7. Możliwość odpytania serwerów RealtimeBlackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.
8. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy.
9. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi.
10. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowania maila do konkretnej skrzynki pocztowej.
11. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością.
12. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.

## Konsola zdalnej administracji

1. Dwa typy konsoli administracyjnej:
* Konsola Cloud – serwer administracyjny po stronie producenta
* Konsola On-premise – lokalny serwer administracyjny
1. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.
2. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego.
3. Możliwość integracji Domeny Active Directory w obu typach konsoli.
4. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
5. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
6. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi
7. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.
8. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
9. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
10. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.
11. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
12. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv
13. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.
14. Możliwość generowania raportu co godzinę.
15. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.
16. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
17. Możliwość dodania etykiety do stacji roboczej.
18. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
19. Możliwość przechowywania kwarantanny maksymalnie 180 dni
20. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
21. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
22. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.
23. Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym.2
24. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.
25. Możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
26. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia lokalizacji na podstawie
* Zakres adresów IP/IP
* Adres bramy
* Adres serwera WINS
* Adres serwera DNS
* Połączenie DHCP sufiksów DNS
* Punkt końcowy może rozwiązać hosta
* Typ sieci
* Nazwa hosta
1. Integracja z serwerem Syslog2
2. Uwierzytelnienie dwuskładnikowe realizowane wyłącznie przez aplikację Google Authenticator
3. Możliwośc ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni1
4. Możliwość zablokowania konta w konsoli jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem1
5. Funkcja pojedynczego logowania – Single Sign-on (SSO)1
6. Możliwość naprawy instalacji z poziomu konsoli1
7. Raport streszczający1 - Możliwość podglądu raportu który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:
* Zarządzane punkty końcowe
* Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne
* Pięć najczęściej blokowanych zagrożeń
* Podział zagrożeń na urządzenia takie jak stacje robocze i serwery
* Status incydentów bezpieczeństwa które wystąpiły
* Stan modułów punktów końcowych
* Ocena ryzyka firmy
* Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.
* Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware
1. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:
* Pakiety
* Sieć
* Kwarantanna
* Licencjonowanie
* Integracje
* Polityki
* Raporty
* Konta
* Firmy
1. Możliwość utworzenia reguły która będzie usuwała punkty końcowe z konsoli zarządzającej jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn które automatycznie będą usuwane oraz pozwala na okrślenie godziny kiedy te maszyny będą usuwane
2. Możliwość określenia własnego serwera NTP2
3. Integracja z vCenter Server2
4. Integracja z Xen Server2
5. Integracja z nutanixPrism Element2
6. Możliwość integracji z Amazon EC2
7. Intergracja z Azure2
8. Każdy z rodzajów ochrony musi być rozdzielony w osobnych oknach konfiguracyjnych, komputery fizyczne, Urządzenia mobilne.
9. Serwer centralnej administracji musi posiadać funkcje przełączenia się miedzy widokiem maszyn fizycznych i urządzeń mobilnych. Tak by wyświetlana była jedynie wskazana grupa urządzeń chronionych.
10. Tworzenie osobnych polityk dla fizycznych komputerów, urządzeń mobilnych oraz maszyn wirtualnych.
11. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
12. Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.
13. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej.
14. Pion firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej
15. Funkcja kontroli aplikacji która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów
16. Funkcja kontroli aplikacji może działać w trybie testowym lub produkcyjnym
17. Funkcja kontroli aplikacji pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat. (2)
18. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
19. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
20. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS
21. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym.
22. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
23. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS
24. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1
25. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych(1).
26. Możliwość skanowania SSL dla połączeń RDP(1)
27. Oprogramowanie umożliwia ochronę kontenerów instalowaną bezpośrednio na hoście kontenera oferuje wgląd w złośliwą aktywność serwera Linux i kontenerów w czasie rzeczywistym.

## Komponenty EDR

1. Czujnik EDR, który gromadzi i przetwarza dane w celu raportowania danych dotyczących punktu końcowego i zachowania aplikacji.
2. Security Analytics, komponent służący do interpretacji metadanych gromadzonych przez czujnik EDR.
3. Możliwość instalacji dodatkowego, lekkiego agenta z czujnikiem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną ochronę. Agent posiada też ochronę urządzenia i ruchu sieciowego oraz filtr stron internetowych.
4. Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności.
* Bazowanie na systemach bazujących na wskaźnikach ataku MITRE i własnej inteligencji.
* Zgłaszanie wszystkich naruszeń jako incydent w module EDR.
1. Badanie incydentów i wizualizacja
* Produkt zapewnia wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym przedziale czasu.
* Produkt integruje się z bazą wiedzy ATT & CK firmy MITRE i odpowiednio oznacza zdarzenia bezpieczeństwa.
* Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi informacjami lub działaniami.
1. Oprogramowanie musi pozwalać na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i linii zdarzeń oraz daje możliwość:
* Filtrowania zdarzeń
* Blokowania procesów
* Dodawanie procesów do czarnej listy
* Dodawanie procesów do białej listy
* Izolacja hosta
* Aktualizacja oprogramowania firm trzecich na hoście (wymagany add-on)
* Przesłanie pliku do Sandbox
* Sprawdzenie informacji o pliku w Google
* Sprawdzenie informacji o pliku w VirusTotal
1. Filtrowanie zdarzeń musi odbywać się na podstawie:
* Ocena zagrożenia od 10 do 100 punktów
* Data wykrycia
* Status
* ID
* Nazwa punktu końcowego
* Typ ataku
1. Wyszukiwanie zdarzeń musi odbywać się na podstawie:
* Nazwa alertu
* IP punktu końcowego
* Hash MD5
* Hash SHA256
* Nazwa użytkownika

## Dostawa, wdrożenie, wsparcie techniczne i szkolenie

1. Wymagane jest aby producent zapewniał wsparcie techniczne minimum przez: telefon, e-mail, czat na żywo oraz zdalne połączenie przez okres minimum 3lat
2. Minimalna liczba licencji to 501 sztuk
3. Instalacja oprogramowania na wskazanym serwerze.
4. Wykonawca przeprowadzi szkolenie administracyjne dla minimum 7 osób