Załącznik nr 2 do zapytania ofertowego

Szczegółowa specyfikacja techniczna

	System
Konstrukcja	System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania. Rozwiązanie powinno być wyposażone w moduł kryptograficzny zgodny ze standardem FIPS 140-2. Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca) Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie HA Active-Passive lub Active-Active. System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej. Rozwiązanie powinno być wyposażone w wysokowydajny wielordzeniowy procesor x86 (CPU) oraz dodatkowo w procesor (NPU) do akceleracji ruchu dla warstwy aplikacji. Rozwiązanie musi być wyposażone w co najmniej jeden dysk SSD służący m.in. do przechowywania logów i raportów bezpośrednio na urządzeniu. Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy. Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB). Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie. Wbudowany port USB umożliwiający podłączenie pamięci flash i przeprowadzenie konfiguracji w trybie Zero Touch. Możliwość rozbudowy o dodatkowe moduły interfejsów sieciowych.
	Specyfikacja techniczna: Pamięć operacyjna RAM nie mniej niż (GB): 6 Przestrzeń do przechowywania logów i raportów nie mniej niż (GB): 64 Liczba fizycznych interfejsów Gigabit Ethernet nie mniej niż: 12 Liczba fizycznych interfejsów SFP Fiber: 2 **Wydajność** Wydajność Firewall nie mniej niż (Mbps): 10000 Wydajność Firewall IMIX nie mniej niż (Mbps): 4000 Wydajność IPS nie mniej niż (Mbps): 2500 Wydajność FW+IPS+AV nie mniej niż (Mbps): 900 Wydajność NGFW nie mniej niż (Mbps): 2500 Liczba równoczesnych połączeń nie mniejsza niż: 5000000 Liczba nowych połączeń na sekundę nie mniejsza niż: 65000 Wydajność IPsec VPN nie mniej niż (Mbps): 4000 Wydajność dla inspekcji ruchu SSL/TLS nie mniej niż (Mbps): 750 Liczba równoczesnych połączeń SSL/TLS nie mniejsza niż: 12000 Liczba równoczesnych tuneli SSL VPN nie mniejsza niż: 1500
Zarządzanie	Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN.

	Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter. Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP. Rozwiązanie powinno oferować wiersz poleceń dostępny z poziomu graficznego interfejsu administratora, portu konsolowego oraz za pośrednictwem protokołu SSH z uwierzytelnianiem przy użyciu kluczy RSA, DSA lub ECDSA o długości min. 2048 bitów. Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora. Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog). Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej. System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS). Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta. System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpwiednika). System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia. System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta, przy czym w podstawowej wersji utrzymywany i udostępniany jest on bezpłatnie i nie wymaga zakupu osobnych subskrypcji. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP, via email jak i dodatkowo do centralnego systemu zarządzania w chmurze. Rozwiązanie powinno oferować wbudowany mechanizm pozwalający na automatyczne tworzenie szyfrowanych hasłem kopii zapasowych konfiguracji w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu. Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich. Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej. Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu licencyjnego a synchronizacja subskrypcji powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania

	systemowego (firmware). Informacja o dostępności nowej wersji powinna pojawiać się w Web GUI. Producent powinien oferować mechanizm automatycznego łatania wykrytych w oprogramowaniu systemowym podatności przez tzw. hotfixies, przy czym administrator powinien móc funkcjonalność tą wyłączyć. Rozwiązanie powinno oferować mechanizm szyfrowania danych takich jak loginy, hasła, klucze które przechowywane są w konifiguracji urządzenia. Dane powinny być zabezpieczone dedykowanym kluczem szyfrującym tworzonym na podstawie bezpiecznie składowanego poza urządzeniem hasła. Rozwiązanie powinno zapewniać możliwość zmiany nazw interfejsów sieciowych.
	Zapora sieciowa, konfiguracja sieciowa oraz routing
Zapora sieciowa	Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection. System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6. Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas. System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. System powinien pozwalać na selektywne wyłączanie reguł zapory sieciowej (bez konieczności ich usuwania). System powinien pozwalać na grupowanie reguł zapory. Wymagana jest funkcjonalność automatycznego wiązania nowotworzonych reguł do właściwych grup na podstawie kryteriów opisujących grupę. Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej. System ochrony powinien zawierać predefiniowane strefy zapory typu: LAN, WAN, DMZ, VPN. Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej. System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). Rozwiązanie powinno oferować narzędzie do symulowanego testu reguł zapory w oparciu o zadane przez administratora kryteria takie jak IP, strefa zapory, użytkownik, dzień, godzina. System powinien pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika.
Trasowanie ruchu	Rozwiązanie powinno oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing. Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów. Rozwiązanie powinno umożliwiać rozkładanie ruchu w oparciu o wagi interfejsów WAN. Rozwiązanie powinno zapewniać obsługę routingu statycznego dla ruchu unicast i multicast. Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM). Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6.
Translacja adresów i portów	Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT. Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT Rozwiązanie powinno pozwalać na automatyczne tworzenie reguł NAT typu loopback czy reflexive rule.
Kształtowanie pasma i jakość usług	System powinien zapewniać możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji. Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne. System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. Podczas klasyfikacji usług rozwiązanie powinno uwzględniać wartości Differentiated Services

	Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6. Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet (od 1 Business Critical do 7 Best Effort).
Podstawowa ochrona przed atakami DoS i DDoS	System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection).
Pozostałe	Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP. Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge). System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. System powinien oferować wsparcie dla IEEE 802.3Q VLAN z możliwością konfiguracji niezależnych puli DHCP. Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). System powinien oferować wsparcie dla usług Dynamic DNS takich jak np.. DynDNS, ZoneEdit, EasyDNS, DynAcces itp. Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd). Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo). Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych.
Kontroler sieci bezprzewodowej	System powinien zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania. Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Access Point, Wireless Bridge oraz Wireless Repeater. Uruchomienie punktów dostępowych sieci bezprzewodowej powinno odbywać się na zasadzie plug-and-play, gdzie punkty dostępowe powinny automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu. Zarządzanie punktami dostępowymi sieci bezprzewodowej powinno odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej. Rozgłaszane sieci bezprzewodowe powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując przy tym możliwość izolacji klientów sieci bezprzewodowej. Rozwiązanie powinno umożliwiać rozgłaszanie wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej (Hide SSID). Rozwiązanie powinno oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise. Rozwiązanie powinno zapewniać wsparcie dla uwierzytelniania klientów w oparciu o IEEE 802.1X (RADIUS Authentication). Rozwiązanie powinno oferować wsparcie dla IEEE 802.11r (Fast Transition). System powinien umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów. Dostęp do sieci bezprzewodowej powinien być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości. System powinien zapewniać możliwość tworzenia odseparowanej sieci dla gości w wariancie walled garden. System powinien pozwalać na rozgłaszanie sieci bezprzedowodych w oparciu o harmonogramy czasowe. Rozwiązanie powinno zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych (Rogue AP detection).
Uwierzytelnianie i obsługa użytkowników	Wymagane uwierzytelniaine użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta. Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników. System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+.

	Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory. System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm). Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server. System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu.
Koncentrator VPN	System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2. System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519). System musi obsługiwać połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN. Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN. Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback. Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego. Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth. Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połaczeń IPsec client-to-site VPN jak i SSL client-to-site VPN. Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN. Urządzenie musi obsługiwać połączenia L2TP over IPsec. Połączenia VPN terminowane muszą być dedykowanej strefie zapory sieciowej.
Logowanie i raportowanie	System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym. System powinien umożliwiać składowanie oraz archiwizację logów. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali. System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących. Rozwiązanie powinno umożliwiać wysyłanie raportów via email. Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV. Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog. System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza. System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację. Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach. System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora.
Intrusion Prevention System	Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur. Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.

i Advanced Threat Protection	Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS. Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS. System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet.
Ochrona przed Malware	Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP. Rozwiązanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania. Dodatkowo rozwiązanie powinno umożliwiać uruchomienie silnika antywirusowego firmy trzeciej. Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń. System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek. Rozwiązanie musi przeprowadzać emulację skryptów Java. Rozwiązanie powinno przeprowadzać tzw. live-lookups t.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta. Rozwiązanie powinno umożliwiać blokowanie potencjalnie niechcianych aplikacji (tzw. Potentially Unwanted Applications - PUAs) System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates)
Inspecja ruchu SSL/TLS	Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów. Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2. Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP. Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443). Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web. Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen.
Filtr Web	Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron Web oraz umożliwiać dodawanie własnych kategorii stron. Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy. Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól. System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowamoa treści komunikatu w tym dodania logo organizacji. Rozwiązanie powinno umożliwiać filtrowanie stron web analzując ich zawartość wykorzystując tzw. Content Filtering na bazie haseł kluczowych. Rozwiązanie powinno oferować ochronę przed Pharmingiem.
Ochrona przed nieznanymi zagrożeniami	Rozwiązanie klasy Sanbox do ochrony przez zadrożeniami typu Zero-Day. Rozwiązanie oferujące statyczną i dynamiczną analizę kodu przesyłanego w ramach ruchu web czy email. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf. Rozwiązanie umożliwiające dodatkową inspekcję i detoancję archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab. System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows i MacOS. System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu.

	System zapewniający analizę strukury kodu w tym analizę przeprowadzaną przez mechanizmy głębokiego uczenia maszynowego. System zapewniający ochronę przed exploitami i złośliwym kodem ransomware. System badający reputację pliku w zewnętrznych bazach takich jak np.Virustotal. System powinien oferować szczegółowe raporty dowodzące przeprowadznie analizy dla w/w mechanizmów.

Ochrona antywirusowa:

Administracja zdalna	1. Rozwiązanie Centralnej administracji musi wspierać instalację na systemach Windows Server, Linux lub być dostępne jako chmurowa usługa producenta. 2. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. 3. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami. 4. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, antyransomware, exploit protection, IPS które działają na stacjach roboczych w sieci. 5. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 6. Rozwiązanie musi zapewniać korzystanie z szablonów raportów, przygotowanych przez producenta. 7. Rozwiązanie musi zapewniać podział uprawnień administracyjnych. 8. Maszyny z systemami Windows, Mac i Linux muszą być zarządzane z jednej konsoli zarządzania. 9. Musi mieć możliwość na synchronizację użytkowników/grup/komputerów z lokalnych serwerów Active Directory w celu zarządzania politykami. 10. Tworzone polityki powinny mieć możliwość zastosowania do użytkowników lub urządzeń. 11. Aktualizacja punktów końcowych powinna mieć możliwość ustawienia przepustowości używanej zarówno do aktualizacji oprogramowania, jak i aktualizacji definicji zagrożeń. 12. Rozwiązanie musi mieć możliwość integracji z interfejsem API zgodne z REST.
Ochrona stacji roboczych	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 8/Windows 8.1/Windows 10/Windows 11). 2. Rozwiązanie musi zapewniać wykrywanie i usuwanie znanego, jak i niespotykanemu wcześniej złośliwemu oprogramowaniu, podobnie musi być w stanie blokować złośliwe oprogramowanie przed jego uruchomieniem. 3. Rozwiązanie musi klasyfikować pliki jako złośliwe, potencjalnie niechciane aplikacje (PUA) lub niegroźne. 4. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 5. Rozwiązanie musi zapewniać wykonywanie skanowania zagrożeń Dni Zero (0 day) w trybie offline (bez dostępu do Internetu). 6. Rozwiązanie musi chronić system nawet w trybie offline i nie będzie polegać na sygnaturach. 7. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych. 8. Rozwiązanie musi mieć możliwość wywołania czyszczenia stacji po każdym aktywnym wykryciu exploita lub ransomware w oparciu o pliki i procesy. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie sumy kontrolnej (SHA1) oraz lokalizacji. 10. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów minimum HTTPS bez konieczności dystrybuowania certyfikatów. 11. Rozwiązanie musi posiadać wbudowany moduł zapobieganie/ograniczania luk w zabezpieczeniach minimum w oparciu o ochrona wykonywania danych (DEP), randomizację układu przestrzeni adresowej (ASLR), Strukturalna ochrona przed

	nadpisaniem obsługi wyjątków (SEHOP), DLL Hijacking, Reflective DLL Injection, Stack Pivot, Dynamic Shellcode. 12. Rozwiązanie musi zapewniać ochronę przed atakami przepełnienia bufora. 13. Rozwiązanie musi być w stanie skanować ruch w oparciu o inspekcję pakietów (IPS) na najniższym poziomie i blokować zagrożenia przed uszkodzeniem systemu operacyjnego lub aplikacji. 14. Rozwiązanie musi mieć możliwość przywrócenia zaszyfrowanych plików do stanu sprzed zaszyfrowania i przywróci je do ich pierwotnej lokalizacji. 15. Rozwiązanie musi zapewnić wykrywanie komunikacji między komputerami końcowymi a serwerami dowodzenia i kontroli biorącymi udział w atakach botnetowych lub innych złośliwych programach. 16. Rozwiązanie musi umożliwiać zarówno ochrona Anti-Exploit, jak i Ransomware bez konieczności łączenia z zewnętrzną usługa „Sandboxing” 17. Rozwiązanie musi chronić przed złośliwym kodem (na przykład skryptami PowerShell) za pomocą interfejsu Microsoft Antimalware Scan Interface (AMSI). 18. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, urządzeń Bluetooth, modemów. 19. Rozwiązanie musi być w stanie wykrywać i blokować kategorie aplikacji, które mogą nie być odpowiednie do użytku w środowisku przedsiębiorstw. 20. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych tzw. URL Filtering. 21. Rozwiązanie musi być w stanie monitorować i konfigurować Zaporę systemu Windows na zarządzanych komputerach i serwerach przy użyciu zasad Zapory systemu Windows. 22. Rozwiązanie musi mieć opcję generowania migawki kryminalistycznej złośliwej aktywności, która wystąpiła na chronionym punkcie końcowym. 23. Rozwiązanie musi posiadać opcję „automatycznego izolowania” skompromitowanych punktów końcowych od sieci. 24. Rozwiązanie musi mieć możliwość monitorowania lub zatrzymywania lokalnych użytkowników administracyjnych lub złośliwych procesów w celu wyłączenia ochrony punktu końcowego: - Zatrzymywanie usług z interfejsu usług - Zabicia usługi i procesu z interfejsu Menedżera zadań - Zmianę konfigurację usługi w interfejsie usług - Odinstalowania - Usunięcia lub modyfikacji chronionych plików lub folderów - Usunięcia lub modyfikacji chronionych kluczy rejestru 25. Rozwiązanie musi mieć możliwość zidentyfikowania, „co się stało, skąd pochodziło naruszenie, jakie pliki zostały naruszone”, oraz dostarczać wskazówek, jak wzmocnić postawę bezpieczeństwa organizacji. 26. Rozwiązanie musi zapewniać widok wszystkiego, co miało wpływ na atak. Pozycje można filtrować według typu. np. pliki, procesy, klucze rejestru. Administrator może przeglądać informacje o każdej pozycji m.in. Nazwa pliku (plik ofiary lub agent złośliwego oprogramowania), identyfikator procesu, znacznik czasu rozpoczęcia/zatrzymania zdarzenia. 27. Rozwiązanie musi zapewniać opcję wysłania podejrzanych plików do zewnętrznych mechanizmów producenta w celu dalszej analizy.
Ochrona Serwerów Windows	1. Rozwiązanie musi wspierać systemy operacyjne Windows Server2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server2016, Windows Server2019, Windows Server2022. 2. Rozwiązanie musi zapewniać wykrywanie i usuwanie znanego, jak i niespotykanemu wcześniej złośliwemu oprogramowaniu, podobnie musi być w stanie blokować złośliwe oprogramowanie przed jego uruchomieniem. 3. Rozwiązanie musi klasyfikować pliki jako złośliwe, potencjalnie niechciane aplikacje (PUA) lub niegroźne. 4. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

	5. Rozwiązanie musi zapewniać wykonywanie skanowania zagrożeń Dni Zero (0 day) w trybie offline (bez dostępu do Internetu). 6. Rozwiązanie musi chronić system nawet w trybie offline i nie będzie polegać na sygnaturach. 7. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych. 8. Rozwiązanie musi mieć możliwość wywołania czyszczenia stacji po każdym aktywnym wykryciu exploita lub ransomware w oparciu o pliki i procesy 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie sumy kontrolnej (SHA1) oraz lokalizacji. 10. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów minimum HTTPS bez konieczności dystrybuowania certyfikatów. 11. Rozwiązanie musi posiadać wbudowany moduł zapobieganie/ograniczania luk w zabezpieczeniach minimum w oparciu o ochrona wykonywania danych (DEP), randomizację układu przestrzeni adresowej (ASLR), Strukturalna ochrona przed nadpisaniem obsługi wyjątków (SEHOP), DLL Hijacking, Reflective DLL Injection, Stack Pivot, Dynamic Shellcode. 12. Rozwiązanie musi zapewniać ochronę przed atakami przepełnienia bufora. 13. Rozwiązanie musi być w stanie skanować ruch w oparciu o inspekcję pakietów (IPS) na najniższym poziomie i blokować zagrożenia przed uszkodzeniem systemu operacyjnego lub aplikacji. 14. Rozwiązanie musi mieć możliwość przywrócenia zaszyfrowanych plików do stanu sprzed zaszyfrowania i przywróci je do ich pierwotnej lokalizacji. 15. Rozwiązanie musi zapewnić wykrywanie komunikacji między komputerami końcowymi a serwerami dowodzenia i kontroli biorącymi udział w atakach botnetowych lub innych złośliwych programach. 16. Rozwiązanie musi umożliwiać zarówno ochrona Anti-Exploit, jak i Ransomware bez konieczności łączenia z zewnętrzną usługa „Sandboxing”. 17. Rozwiązanie musi być chronić przed złośliwym kodem (na przykład skryptami PowerShell) za pomocą interfejsu Microsoft Antimalware Scan Interface (AMSI). 18. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, urządzeń Bluetooth, modemów. 19. Rozwiązanie musi być w stanie wykrywać i blokować kategorie aplikacji, które mogą nie być odpowiednie do użytku w środowisku przedsiębiorstw. 20. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych tzw. URL Filtering. 21. Rozwiązanie musi być w stanie monitorować i konfigurować Zaporę systemu Windows na zarządzanych komputerach i serwerach przy użyciu zasad Zapory systemu Windows. 22. Rozwiązanie musi mieć opcję generowania migawki kryminalistycznej złośliwej aktywności, która wystąpiła na chronionym punkcie końcowym. 23. Rozwiązanie musi posiadać opcję „automatycznego izolowania” skompromitowanych punktów końcowych od sieci. 24. Rozwiązanie musi mieć możliwość monitorowania lub zatrzymywania lokalnych użytkowników administracyjnych lub złośliwych procesów w celu wyłączenia ochrony punktu końcowego: - Zatrzymywanie usług z interfejsu usług - Zabicia usługi i procesu z interfejsu Menedżera zadań - Zmianę konfigurację usługi w interfejsie usług - Odinstalowania - Usunięcia lub modyfikacji chronionych plików lub folderów - Usunięcia lub modyfikacji chronionych kluczy rejestru 25. Rozwiązanie musi mieć możliwość zidentyfikowania, „co się stało, skąd pochodziło naruszenie, jakie pliki zostały naruszone”, oraz dostarczać wskazówek, jak wzmocnić postawę bezpieczeństwa organizacji.

	26. Rozwiązanie musi zapewniać widok wszystkiego, co miało wpływ na atak. Pozycje można filtrować według typu. np. pliki, procesy, klucze rejestru. Administrator może przeglądać informacje o każdej pozycji m.in. Nazwa pliku (plik ofiary lub agent złośliwego oprogramowania), identyfikator procesu, znacznik czasu rozpoczęcia/zatrzymania zdarzenia. 27. Rozwiązanie musi zapewniać opcję wysłania podejrzanych plików do zewnętrznych mechanizmów producenta w celu dalszej analizy.
Licencjonowanie	Razem należy dostarczyć: 1. 20 licencji na końcówki klienckie licencjonowane na użytkownika. 2. 1 licencji na serwery windows. 3. Licencje na okres 36 miesięcy (końcówki/serwery). 4. Zaawansowane wsparcie producenta na okres równy okresowi licencjonowania zapewniający: - nielimitowany dostęp do poprawek i aktualizacji, - dostęp do nowych funkcji i funkcjonalności w obrębie modułów licencyjnych, - wsparcie telefoniczne i mailowe producenta w trybie 24 x 7.