Załącznik Nr 2 do SWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA ORAZ WYMAGANIA TECHNICZNE WRAZ Z FORMULARZEM ASORTYMENTOWO-CENOWYM

Lp.	Asortyment	Ilość	Cena jedn. netto	VAT %	Wartość netto	Wartość brutto	Model/typ, Producent, rok produkcji (wszystkich elementów składowych)
1.	**SYSTEM BEZPIECZEŃSTWA – UTM**	1 szt.					
2.	**SYSTEM LOGOWANIA I RAPORTOWANIA**	1 szt.					
3.	**CENTRALNIE ZARZĄDZANY SYSTEM OCHRONY ANTYWIRUSOWEJ Z EDR/XDR WRAZ Z LICENCJAMI**	1 szt.					
Razem wartość netto od poz. 1 do 3							
Razem wartość brutto od poz. 1 do 3							

Lp.	Opis minimalnych wymaganych parametrów technicznych	Parametr wymagany	Parametr oferowany
1. SYSTEM BEZPIECZEŃSTWA – UTM			
Dostarczenie, montaż, konfiguracja, podłączenie do infrastruktury, szkolenie administratorów Zamawiającego			
Wymagania ogólne			
1.	Rok produkcji - 2021/2022	TAK, podać	
2.	Sprzęt fabrycznie nowy, niepowystawowy	TAK, podać	
3.	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub	TAK, podać	

	komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.		
4.	W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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.	TAK, podać	
5.	System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.	TAK, podać	
6.	**<u>SYSTEM BEZPIECZEŃSTWA – UTM</u>:**	TAK, podać	Model, nazwa /nr katalogowy …… Producent …… Kraj pochodzenia ……... Rok produkcji ……
Redundancja, monitoring i wykrywanie awarii:			
7.	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.	TAK, podać	
8.	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.	TAK, podać	
9.	Monitoring stanu realizowanych połączeń VPN.	TAK, podać	
10.	System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.	TAK, podać	
Interfejsy, Dysk, Zasilanie:			
11.	System realizujący funkcję Firewall musi dysponować minimum: • 16 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps. • 2 gniazdami SFP+ 10 Gbps.	TAK, podać	
12.	System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza	TAK, podać	

	USB.		
13.	W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.	TAK, podać	
14.	System musi być wyposażony w zasilanie AC.	TAK, podać	
Parametry wydajnościowe:			
15.	W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę	TAK, podać	
16.	Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.	TAK, podać	
17.	Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.	TAK, podać	
18.	Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps.	TAK, podać	
19.	Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.	TAK, podać	
20.	Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.	TAK, podać	
21.	Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.	TAK, podać	
Funkcje Systemu Bezpieczeństwa: **W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:**			
22.	Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.	TAK, podać	
23.	Kontrola Aplikacji.	TAK, podać	
24.	Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.	TAK, podać	
25.	Ochrona przed malware.	TAK, podać	
26.	Ochrona przed atakami - Intrusion Prevention System.	TAK, podać	
27.	Kontrola stron WWW.	TAK, podać	
28.	Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.	TAK, podać	
29.	Zarządzanie pasmem (QoS, Traffic shaping).	TAK, podać	
30.	Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).	TAK, podać	
31.	Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.	TAK, podać	

32.	Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.	TAK, podać	
33.	Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.	TAK, podać	
34.	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).	TAK, podać	
Polityki, Firewall			
35.	Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.	TAK, podać	
36.	System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP.	TAK, podać	
37.	W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa przynajmniej DMZ, LAN, WAN.	TAK, podać	
38.	Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP.	TAK, podać	
39.	Polityka firewall musi umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.	TAK, podać	
40.	W ramach systemu musi istnieć możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.	TAK, podać	
41.	Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.	TAK, podać	
Połączenia VPN			
42.	System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20.	TAK, podać	

	• 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 oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site.		
43.	System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.	TAK, podać	
Routing i obsługa łączy WAN			
44.	W zakresie routingu rozwiązanie musi zapewniać 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 (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.	TAK, podać	
Funkcje SD-WAN			
45.	System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.	TAK, podać	

46.	SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).	TAK, podać	
Zarządzanie pasmem			
47.	System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.	TAK, podać	
48.	Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.	TAK, podać	
49.	System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.	TAK, podać	
50.	System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.	TAK, podać	
Ochrona przed malware			
51.	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach	TAK, podać	
52.	Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.	TAK, podać	
53.	System musi umożliwiać 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.	TAK, podać	
54.	System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.	TAK, podać	
55.	System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).	TAK, podać	
56.	Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	TAK, podać	
57.	System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.	TAK, podać	
58.	System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	TAK, podać	
59.	Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.	TAK, podać	
60.	Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.	TAK, podać	
Ochrona przed atakami:			
61.	Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.	TAK, podać	

62.	System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.	TAK, podać	
63.	Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora	TAK, podać	
64.	Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.	TAK, podać	
65.	System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS	TAK, podać	
66.	Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies dla protokołu http.	TAK, podać	
67.	Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	TAK, podać	
68.	Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.	TAK, podać	
Kontrola aplikacji			
69.	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.	TAK, podać	
70.	Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	TAK, podać	
71.	Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, takich jak pobieranie, wysyłanie plików.	TAK, podać	
72.	Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.	TAK, podać	
73.	Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	TAK, podać	
74.	Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).	TAK, podać	
75.	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).	TAK, podać	
Kontrola WWW			
76.	Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.	TAK, podać	
77.	W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.	TAK, podać	
78.	Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.	TAK, podać	

79.	Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.	TAK, podać	
80.	Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).	TAK, podać	
81.	Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.	TAK, podać	
82.	Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.	TAK, podać	
83.	Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.	TAK, podać	
84.	W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.	TAK, podać	
Uwierzytelnianie użytkowników w ramach sesji			
85.	System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.	TAK, podać	
86.	Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.	TAK, podać	
87.	Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.	TAK, podać	
88.	Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.	TAK, podać	
Zarządzanie			
89.	Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.	TAK, podać	
90.	Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.	TAK, podać	
91.	Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.	TAK, podać	
92.	System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3	TAK, podać	

	oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.		
93.	System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.	TAK, podać	
94.	Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.	TAK, podać	
95.	Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	TAK, podać	
96.	Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).	TAK, podać	
97.	Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.	TAK, podać	
Logowanie			
98.	Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.	TAK, podać	
99.	W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.	TAK, podać	
100.	Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.	TAK, podać	
101.	Możliwość włączenia logowania per reguła w polityce firewall.	TAK, podać	
102.	Musi istnieć możliwość logowania do serwera SYSLOG.	TAK, podać	
103.	Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.	TAK, podać	
Certyfikaty			
104.	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall	TAK, podać	
Testy wydajnościowe oraz funkcjonalne			
105.	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.	TAK, podać	
Serwisy i licencje			
106.	Licencje upoważniające do korzystania z aktualnych baz	TAK, podać	

	funkcji ochronnych producenta i serwisów (dostarczone wraz ze sprzętem). Powinny one obejmować: • Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [60] miesięcy.		
Opisy do wymagań ogólnych			
107.	W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.	TAK, podać	
108.	Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.	TAK, podać	
Gwarancja oraz wsparcie			
109.	Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres [60] 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.	TAK, podać	
110.	Rozszerzone wsparcie serwisowe AHB: System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [60] miesięcy. 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 Wymagania powinny być potwierdzone dokumentami: • Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o	TAK, podać	

	gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego.		
111.	W ramach przedmiotu zamówienia Wykonawca zapewni szkolenie w formie stacjonarnej lub online dla 2 administratorów, zgodne z dostarczanym rozwiązaniem, zorganizowane w autoryzowanym przez Producenta ośrodku szkoleniowym, potwierdzone certyfikatem Producenta lub autoryzowanego centrum szkoleniowego Producenta.	TAK, podać	
2. SYSTEM LOGOWANIA I RAPORTOWANIA			
Konfiguracja, podłączenie do infrastruktury Zamawiającego			
Wymagania ogólne			
112.	W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.	TAK, podać	
113.	**<u>SYSTEM LOGOWANIA I RAPORTOWANIA</u>:**	TAK, podać	Nazwa /nr katalogowy …… Producent …… Kraj pochodzenia ……
Interfejsy, Dysk, Zasilanie:			
114.	System musi dysponować co najmniej: • 2 portami Gigabit Ethernet RJ-45.	TAK, podać	
115.	Rozwiązanie musi dysponować powierzchnią dyskową min. 4 TB.	TAK, podać	
116.	System musi być wyposażony w zasilanie AC.	TAK, podać	
Parametry wydajnościowe:			
117.	System musi być w stanie przyjmować minimum 25 GB logów na dzień.	TAK, podać	
118.	System musi być w stanie przeanalizować minimum 500 logów na sekundę.	TAK, podać	
119.	Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 50 systemów.	TAK, podać	
W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:			
Logowanie			

120.	Podgląd logowanych zdarzeń w czasie rzeczywistym.	TAK, podać	
121.	Możliwość przeglądania logów historycznych z funkcją filtrowania.	TAK, podać	
122.	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: a. Listę najczęściej wykrywanych ataków. b. Listę najbardziej aktywnych użytkowników. c. Listę najczęściej wykorzystywanych aplikacji. d. Listę najczęściej odwiedzanych stron www. e. Listę krajów , do których nawiązywane są połączenia. f. Listę najczęściej wykorzystywanych polityk Firewall. g. Informacje o realizowanych połączeniach IPSec.	TAK, podać	
123.	Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.	TAK, podać	
124.	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.	TAK, podać	
125.	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.	TAK, podać	
Raportowanie			
126.	Generowanie raportów co najmniej w formatach: PDF, CSV.	TAK, podać	
127.	Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.	TAK, podać	
128.	Funkcję definiowania własnych raportów.	TAK, podać	
129.	Możliwość spolszczenia raportów.	TAK, podać	
130.	Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.	TAK, podać	
Korelacja logów			
131.	Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.	TAK, podać	
132.	Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.	TAK, podać	
133.	Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic.	TAK, podać	

	• Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.		
Zarządzanie			
134.	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. • Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.	TAK, podać	
135.	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.	TAK, podać	
Opisy do wymagań ogólnych			
136.	W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.	TAK, podać	
137.	Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.	TAK, podać	
Gwarancja oraz wsparcie			
138.	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	TAK, podać	
139.	W okresie gwarancyjnym czas reakcji serwisu, tj. od chwili powiadomienia do rozpoczęcia naprawy wyniesie maksymalnie 1 dzień roboczy.	TAK, podać	
140.	Czas skutecznej naprawy max. 5 dni roboczych licząc od dnia zgłoszenia	TAK, podać	
141.	Instrukcje obsługi w języku polskim w wersji elektronicznej dostarczona ze sprzętem	TAK, podać	
142.	Wykonanie w cenie oferty szkolenia 2 administratorów z	TAK, podać	

	działania urządzenia i jej obsługi		
143.	Deklaracja zgodności lub certyfikat CE	TAK, podać	
3. CENTRALNIE ZARZĄDZANY SYSTEM OCHRONY ANTYWIRUSOWEJ Z EDR/XDR WRAZ Z LICENCJAMI			
Dostarczenie, instalacja i konfiguracja, szkolenie administratorów Zamawiającego			
Wymagania ogólne			
144.	W ramach postępowania wymaganym jest dostarczenie, instalacja i konfiguracja, przekazanie licencji centralnie zarządzanego systemu ochrony antywirusowej z zaporą ogniową oraz systemem EDR/XDR **dla 130 szt. stacji roboczych i serwerów oraz urządzeń mobilnych**.	TAK, podać	
145.	**CENTRALNIE ZARZĄDZANY SYSTEM OCHRONY ANTYWIRUSOWEJ Z EDR/XDR:**	TAK, podać	Nazwa i wersja systemu …….. Producent ……
Administracja zdalna:			
146.	Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.	TAK, podać	
147.	Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.	TAK, podać	
148.	Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.	TAK, podać	
149.	Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.	TAK, podać	
150.	Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.	TAK, podać	
151.	Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.	TAK, podać	
152.	Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android.	TAK, podać	
153.	Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.	TAK, podać	
154.	Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio,	TAK, podać	

	drukarki, karty sieciowe, urządzenia masowe).		
155.	Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.	TAK, podać	
156.	Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.	TAK, podać	
157.	Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.	TAK, podać	
158.	Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.	TAK, podać	
159.	Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.	TAK, podać	
160.	Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.	TAK, podać	
161.	Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.	TAK, podać	
Ochrona stacji roboczych:			
162.	Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11).	TAK, podać	
163.	Rozwiązanie musi wspierać architekturę ARM64.	TAK, podać	
164.	Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.	TAK, podać	
165.	Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.	TAK, podać	
166.	Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.	TAK, podać	
167.	Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	TAK, podać	
168.	Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.	TAK, podać	
169.	Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.	TAK, podać	

170.	Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.	TAK, podać	
171.	Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).	TAK, podać	
172.	Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.	TAK, podać	
173.	Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.	TAK, podać	
174.	Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.	TAK, podać	
175.	Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.	TAK, podać	
176.	Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.	TAK, podać	
177.	Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu	TAK, podać	

	operacyjnego, pliku hosts, sterowników.		
178.	Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.	TAK, podać	
179.	Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.	TAK, podać	
180.	Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).	TAK, podać	
181.	Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.	TAK, podać	
182.	Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego MS Outlook.	TAK, podać	
183.	Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: • tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, • tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.	TAK, podać	
184.	Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.	TAK, podać	
185.	Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.	TAK, podać	
186.	Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.	TAK, podać	
187.	Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.	TAK, podać	
188.	Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.	TAK, podać	
189.	Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.	TAK, podać	
190.	W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.	TAK, podać	
Ochrona serwera:			
191.	Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8,	TAK, podać	

	Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux.		
192.	Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.	TAK, podać	
193.	Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.	TAK, podać	
194.	Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.	TAK, podać	
195.	Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.	TAK, podać	
196.	Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.	TAK, podać	
197.	Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.	TAK, podać	
198.	Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.	TAK, podać	
Dodatkowe wymagania dla ochrony serwerów Windows:			
199.	Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.	TAK, podać	
200.	Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).	TAK, podać	
201.	Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.	TAK, podać	
202.	Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.	TAK, podać	
203.	Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.	TAK, podać	
204.	Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.	TAK, podać	
205.	Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.	TAK, podać	
206.	Rozwiązanie musi zapewniać możliwość dodawania	TAK, podać	

	wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.		
207.	Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.	TAK, podać	
Dodatkowe wymagania dla ochrony serwerów Linux:			
208.	Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.	TAK, podać	
209.	Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.	TAK, podać	
210.	Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.	TAK, podać	
211.	Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.	TAK, podać	
Szyfrowanie:			
212.	System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.	TAK, podać	
213.	System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).	TAK, podać	
214.	Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.	TAK, podać	
215.	Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.	TAK, podać	
Endpoint Detection and Response:			
216.	Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS współpracujący z systemem do ochrony stacji roboczych tego samego producenta.	TAK, podać	
217.	Rozwiązanie musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.	TAK, podać	
218.	Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.	TAK, podać	
219.	Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.	TAK, podać	
220.	Rozwiązanie musi zapewniać wykluczenia dotyczące procesu lub procesu „rodzica”.	TAK, podać	
221.	Rozwiązanie musi umożliwiać utworzenie wykluczenia	TAK, podać	

	automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia.		
222.	Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.	TAK, podać	
223.	Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.	TAK, podać	
224.	Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne, pobrania do analizy oraz ich zablokowania.	TAK, podać	
225.	Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł.	TAK, podać	
226.	Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli.	TAK, podać	
227.	Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania poleceń powershell.	TAK, podać	
Ochrona urządzeń mobilnych opartych o system Android:			
228.	Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.	TAK, podać	
229.	Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.	TAK, podać	
230.	Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).	TAK, podać	
231.	Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.	TAK, podać	
232.	Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: a. usunięcie zawartości urządzenia, b. przywrócenie urządzenie do ustawień fabrycznych, c. zablokowania urządzenia, d. uruchomienie sygnału dźwiękowego, e. lokalizację GPS.	TAK, podać	
233.	Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.	TAK, podać	
234.	Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła.	TAK, podać	

Gwarancja i wsparcie:			
235.	Wykonawca zapewni okres gwarancji i usługi wsparcia technicznego na okres 60 m-cy	TAK, podać	
236.	W ramach przedmiotu zamówienia Wykonawca zapewni szkolenie w formie stacjonarnej lub online dla 2 administratorów, zgodne z dostarczanym rozwiązaniem, prowadzone przez autoryzowany ośrodek szkoleniowy dystrybutora rozwiązania w Polsce.	TAK, podać	

UWAGA!
Podane wyżej parametry są wymaganiami minimalnymi dla przedmiotu zamówienia. Niespełnienie któregokolwiek z wymaganych parametrów będzie skutkowało odrzuceniem oferty.

W kolumnie „Parametr oferowany" Wykonawca wpisuje słowo „TAK", jeśli oferowany przedmiot zamówienia spełnia minimalne parametry podane przez Zamawiającego i podaje ten parametr.

W sytuacji zaoferowania przedmiotu zamówienia o parametrach wyższych niż minimalne, oprócz wpisania słowa „TAK" należy je również podać w kolumnie „Parametr oferowany".
W przypadku wyboru oferty Wykonawcy, który zaoferował wyższe niż wymagane parametry, będzie on zobowiązany do dostarczenia Zamawiającemu przedmiotu zamówienia posiadającego te wyższe parametry.

Oświadczam, że oferowane powyżej wyspecyfikowane urządzenie jest fabrycznie nowe, niepowystawowe, kompletne, kompatybilne i będzie gotowe do użytkowania bez żadnych dodatkowych zakupów poza materiałami eksploatacyjnymi.