

„Zakup sprzętu i oprogramowania systemowego dla Gminy Dobra w ramach projektu Cyberbezpieczna Gmina Dobra”

Opis Przedmiotu Zamówienia

Spis treści

Słownik	2
1. Organizacja realizacji zamówienia.....	2
2. Specyfikacja techniczna przedmiotu zamówienia	3
2.1. Dostawa urządzenia klasy NDR wraz z oprogramowaniem 1 szt.	3
2.1.1. Wymagania ogólne w zakresie dostawy sprzętu	10
2.2. Urządzenie typu Firewall UTM z oprogramowaniem SSL VPN 1 szt.	10
2.3. Zakup oprogramowania na potrzeby SSL/VPN	23
2.4. Przetączniki sieciowe 6 szt.....	24
2.5. Rozwiązanie do Backup'u	28
2.6. Oprogramowanie antywirusowe z modułem ochrony prewencyjnej - 75 licencji	38

Słownik

L.P	Pojęcie	Opis
1.	Zamawiający	Gmina Dobra 34-642 Dobra 233 Reprezentowana przez Urząd Gminy Dobra 34-642 Dobra 233

1. Organizacja realizacji zamówienia

- 1) Komunikacja w ramach niniejszego zamówienia oraz podczas jego realizacji może odbywać się telefonicznie, poprzez komunikatory, ale wszelkie uzgodnienia w zakresie realizacji przedmiotu muszą być uzgadniane pomiędzy stronami pisemnie, w tym elektronicznie, poprzez wymianę informacji pocztą elektroniczną na wskazane adresy email.
- 2) Realizacja przedmiotu zamówienia odbywać się będzie zdalnie oraz lokalnie w zakresie właściwym dla zadania. Realizacja zleconych zadań może wymagać w uzasadnionych przypadkach obecności Wykonawcy w siedzibie Zamawiających nawet jeżeli określono realizację zdalną wybranego zakresu, jeżeli zdalna realizacja będzie niemożliwa lub może negatywnie wpływać na jakość wykonania przedmiotu projektu.
- 3) Wykonawca musi przekazywać w trakcie realizacji czynności przewidzianych niniejszym zamówieniem informacje o wszelkich wykrytych podatnościach, w celu umożliwienia Zamawiającemu podjęcia natychmiastowych działań naprawczych.
- 4) Wykonawca każdorazowo, winien uzgadniać z Zamawiającym termin prowadzenia bardziej inwazyjnych czynności ze szczególnym uwzględnieniem: DoS, i prowadzić je dopiero po uzyskaniu pisemnej, w tym poprzez środki elektronicznej komunikacji, zgody osoby Zamawiającego. Wykonawca musi prowadzić prace, które umożliwią mu zakończenie w każdym momencie takich testów.
- 5) Jakiegokolwiek czynności prowadzone przez Wykonawcę nie mogą spowodować przestoju w świadczeniu usług przez Zamawiającego. Gdyby jednak przeprowadzenie testów rodziło ryzyko przestoju w pracy, Wykonawca w porozumieniu z Zamawiającym Wykonawcą opracuje, zaakceptowany przez Zamawiającego, scenariusz alternatywny przeprowadzenia testów tak aby zminimalizować ryzyko problemów.
- 6) Wykonawca może prowadzić prace po uprzednim uzgodnieniu ich zakresu z każdym z Zamawiających. Przez uzgodnienie należy rozumieć precyzyjne wskazanie daty oraz czasu rozpoczęcia a także zakończenia prac.
- 7) Wykonawca ma obowiązek ścisłej współpracy z Zamawiającym na każdym etapie realizacji zamówienia.
- 8) Wykonawca winien uwzględniać wszelkie uwagi Zamawiającego, które doprecyzowują lub uzupełniają zapisy w zapytaniu ofertowym i nie są z nimi sprzeczne.
- 9) Zamawiający we współpracy z Wykonawcą ustalą harmonogram spotkań mających na celu weryfikację stanu projektu. Zakłada się minimalną częstotliwość spotkań raz w tygodniu.
- 10) Wykonawca musi dostosować się do polityk bezpieczeństwa Zamawiającego.

2. Specyfikacja techniczna przedmiotu zamówienia

2.1. Dostawa urządzenia klasy NDR wraz z oprogramowaniem 1 szt.

Parametr	Opis
Elementy systemu bezpieczeństwa	<ul style="list-style-type: none"> Wysokość 1U do montażu w szafie rack. Posiadać co najmniej dwa porty USB Urządzenie musi posiadać dedykowany port do zarządzania Urządzenie musi posiadać minimum interfejsów: 2x SFP+, 8x SFP, 8x GE Musi obsługiwać co najmniej 1T przestrzeni dyskowej. Minimum 1 Gb/s przepustowości wykrywania naruszeń w dwukierunkowym ruchu HTTP z włączonymi wszystkimi funkcjami wykrywania zagrożeń Proponowane rozwiązanie musi obsługiwać minimum 750 tys. jednocześnie sesji. Proponowane rozwiązanie musi obsługiwać 32000 nowych sesji /s w ruchu HTTP.
Usługi sieciowe	<ul style="list-style-type: none"> Musi obsługiwać pasywny tryb pracy (TAP), nie ingerując w sieć klienta. Rozwiązanie musi być w stanie zintegrować się z zaporami ogniowymi tej samej marki w celu ograniczenia zagrożeń Musi posiadać możliwość rozwiązywania wiadomości przez protokół MPLS, VXLAN oraz QinQ i wykrywania zagrożeń w tych wiadomościach.
Kontrola aplikacji	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka oraz wspierać komunikatory internetowe, p2p, pocztę e-mail, przesyłanie plików, gry online, strumieniowe przesyłanie multimediów itp. Rozwiązanie musi być w stanie zidentyfikować aplikacje mobilne typu iOS lub Android. Rozwiązanie musi być w stanie identyfikować aplikacje w chmurze, musi zapewniać wielowymiarowe monitorowanie i statystyki dla aplikacji w chmurze, w tym kategorię ryzyka i funkcje.
Wykrywanie zagrożeń	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać co najmniej 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, ręczne i automatyczne aktualizacje, wyodrębnianie sygnatur oraz wbudowaną encyklopedię zagrożeń. Rozwiązanie musi obsługiwać ochronę przed atakami SQL injection, XSS, buffer overflow zarówno dla IPv4 jak i IPv6 Rozwiązanie powinno obsługiwać ochronę przed atakami C&C z limitem żądań, limitem proxy, niestandardowym

Parametr	Opis
	<p>progiem, Musi obsługiwać wykrywanie co najmniej metod uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA</p> <ul style="list-style-type: none"> Rozwiązanie musi obsługiwać wykrywanie anomalii protokołów HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS itp. Niestandardowe reguły wykrywania włamań muszą obsługiwać konfigurowanie kierunku ruchu ataku w celu poprawy dokładności analizy źródła ataku. Rozwiązanie powinno umożliwiać tworzenie białych list dla modułu IPS. Rozwiązanie musi mieć wstępnie zdefiniowane profile IPS. Rozwiązanie musi mieć opcję przechwytywania pakietów Rozwiązanie musi umieć wykrywać reverse-shell Rozwiązanie potrafi zdefiniować odpowiednie treshholdy chroniące przed atakami Flood, bazując na parametrach dostarczonego ruchu System musi mapować wykryte zagrożenia na framework MITRE ATT&CK
Skanowanie antywirusowe	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać co najmniej 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur. Rozwiązanie musi wspierać antywirus oparty na przepływie dla protokołów min. HTTP, SMTP, POP3, IMAP, FTP/SFTP. Rozwiązanie musi obsługiwać wykrywanie zaszyfrowanych skompresowanych plików. Rozwiązanie powinno obsługiwać wykrywanie wirusów w skompresowanych plikach, takich jak RAR, ZIP, GZIP, BZIP2, TAR oraz wspierać wielowarstwowe wykrywanie skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji po wykryciu zagrożenia w tych plikach
Wykrywanie botnetów C&C	<ul style="list-style-type: none"> Rozwiązanie powinno wspierać skuteczne wykrywanie botów intranetowych i zapobieganie dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównywanie uzyskanych informacji z bazą adresów C&C. Rozwiązanie musi obsługiwać automatyczną aktualizację sygnatur botnetów C&C Rozwiązanie musi obsługiwać dwa typy bazy adresów C&C: bazę adresów IP i bazę danych domen. Rozwiązanie musi obsługiwać wykrywanie C&C protokołów w protokołach TCP, HTTP i DNS. Rozwiązanie musi wspierać włączenie wykrywania DGA w celu analizy odpowiedzi DNS i wykrywania, czy urządzenie jest atakowane przez nazwę domeny DGA.

Parametr	Opis
	<ul style="list-style-type: none"> Musi wspierać wykrywanie tunelowania w protokole DNS w tym analizowanie zapytań DNS a także rejestrować logów zagrożeń wykrytych tuneli DNS.
Sandbox w chmurze	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać oparte na chmurze wirtualne środowisko analizy złośliwego oprogramowania w celu znalezienia nieznanymi zagrożeń Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do piaskownicy w chmurze w celu analizy. Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów, w tym HTTP/HTTPS, POP3, IMAP4, SMTP i FTP. Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR, SWF oraz skrypty Rozwiązanie powinno dostarczyć kompletny raport analizy behawioralnej dla złośliwych plików. Rozwiązanie musi obsługiwać globalne udostępnianie informacji o zagrożeniach, aby wykryć nowe nieznanne zagrożenie.
Wykrywanie spamu	<ul style="list-style-type: none"> Rozwiązanie musi wspierać klasyfikację i wykrywanie spamu w czasie rzeczywistym Rozwiązanie musi obsługiwać wykrywanie spamu niezależnie od języka, formatu lub treści wiadomości. Rozwiązanie musi obsługiwać protokoły poczty e-mail smtp i pop3 Rozwiązanie musi obsługiwać białe listy wiadomości e-mail z zaufanych domen.
Dodatkowe funkcje ochrony	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać wykrywanie DoS / DDoS, SYN Flood, DNS query flood itp. Rozwiązanie musi obsługiwać wykrywanie ataków ARP w tym spoofing ARP. Rozwiązanie musi obsługiwać wykrywanie anormalnych ataków protokołu. Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu pop
Inteligentne funkcje bezpieczeństwa	<ul style="list-style-type: none"> Rozwiązanie powinno obsługiwać analizę korelacji zagrożeń, korelację między nieznanymi zagrożeniami, nietypowym zachowaniem i zachowaniem aplikacji, aby wykryć potencjalne zagrożenia lub ataki. Rozwiązanie powinno umożliwiać aktualizację bazy danych modelu zachowania szkodliwego oprogramowania online w czasie rzeczywistym.

Parametr	Opis
	<ul style="list-style-type: none"> Rozwiązanie powinno obsługiwać wykrywanie ponad 2000 znanych i nieznanych rodzin złośliwego oprogramowania, w tym wirusów, robaków, trojanów itp. Rozwiązanie musi obsługiwać zaawansowane wykrywanie złośliwego oprogramowania oparte na obserwacji zachowania Rozwiązanie musi wspierać wykrycia oprogramowania ransomware i złośliwego oprogramowania do wydobywania kryptowalut. Rozwiązanie powinno obsługiwać modelowanie zachowania w oparciu o ruch bazowy L3-L7, aby ujawnić nietypowe zachowanie sieci, takie jak skanowanie HTTP, Spider, SPAM, słabe hasła SSH / FTP dla serwerów i hostów. Rozwiązanie musi obsługiwać wykrywanie DDoS, w tym Flood, Sockstress, zip of death, reflect, dns query, SSL DDos i aplikacyjny DDoS Rozwiązanie musi obsługiwać inspekcję zaszyfrowanego ruchu tunelowego dla nieznanych aplikacji Rozwiązanie musi obsługiwać aktualizację bazy danych modelu nieprawidłowego zachowania online w czasie rzeczywistym Rozwiązanie musi zapewniać analizę kryminalistyczną, w tym analizę zagrożeń, bazę wiedzy, historię i topologię zagrożeń. Rozwiązanie musi obsługiwać działania administratora w celu zmiany stanu zagrożenia na false positive, naprawionego, zignorowanego, potwierdzonego zdarzenia Rozwiązanie musi obsługiwać czyszczenie zagrożeń serwera jednym kliknięciem i ponowną ocenę bezpieczeństwa hosta Rozwiązanie powinno obsługiwać białą listę zagrożeń, w tym nazwę zagrożenia, źródłowy/docelowy adres IP, liczbę odwiedzin itd. Rozwiązanie musi obsługiwać przechwytywanie pakietów online Rozwiązanie musi obsługiwać lokalną technologię honeypot, aby wychwytywać ataki zagrożeń sieciowych i potwierdzać źródło zagrożenia, typ zagrożenia i częstotliwość występowania Rozwiązanie musi obsługiwać wykrywanie oszustw na podstawie behawioralnej dla ftp, HTTP, MYSQL, SSH, TELNET, dokumentów lub baz danych

Parametr	Opis
	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać funkcję polowania na zagrożenia (threat hunting), aby zebrać kompleksowe dowody i zapewnić dogłębną analizę Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force remote dekho, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu poprawy wykrywalności funkcji śledzenia zagrożeń.
Widoczność ryzyka/zagrożeń	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać wizualizację zagrożeń intranetowych dla serwerów (zasobów krytycznych), a także wykrywanie nietypowego ruchu z nimi związanego. Rozwiązanie musi obsługiwać widoczność zagrożeń dla ryzykownych hostów, w tym nazwy hosta, systemu operacyjnego, przeglądarki, typu usługi, aby rejestrować zagrożenia hosta i nietypowy ruch. Rozwiązanie musi obsługiwać widoczność podstawowych informacji opartych na hoście, indeksu ryzyka, zagrożeń i nietypowego ruchu. Rozwiązanie powinno wspierać widoczność zagrożeń, w tym nazwę zagrożenia, typ zagrożenia, poziom ryzyka, bazę wiedzy, pakiet kryminalistyczny itp. Rozwiązanie powinno dostarczyć wszystkie statystyki klasyfikacji zdarzeń zagrożeń w oparciu o IOC i trend zdarzeń zagrożeń w ciągu co najmniej 2 tygodni. Rozwiązanie musi wspierać wskazanie ścieżki ataku.
Analiza i odpowiedzi na incydenty	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać aktualizację w czasie rzeczywistym najpoważniejszych informacji o zagrożeniach znalezionych w branży do urządzenia z chmury Obsługa wyświetlania najnowszych informacji o zagrożeniach w wyskakujących okienkach. Obsługa rejestrowania i sprawdzania, czy w sieci wystąpiło odpowiednie zagrożenie. Pomoc techniczna w celu dostarczenia szczegółowych informacji o zagrożeniach i sugestii dotyczących rozwiązania. Wsparcie konfigurowania reguł ostrzegania o zagrożeniach, w tym warunków zagrożenia i metody działania, które w przypadku wystąpienia zdarzenia stanowiącego zagrożenie, system powiadomi użytkownika lub podejmie odpowiedź w odpowiednim czasie zgodnie z metodą działania określoną w regule (np. połączenie z firewall, przypomnienie głosowe lub wysłanie pocztą e-mail.

Parametr	Opis
Administracja	<ul style="list-style-type: none"> Rozwiązanie musi mieć zintegrowany sieciowy interfejs użytkownika (WebUI) i interfejs wiersza poleceń (CLI) Rozwiązanie powinno obsługiwać zarządzanie dostępem z HTTP/HTTPS, SSH, telnet, konsoli Rozwiązanie musi być w stanie chronić system przed atakami brute-force na nazwę użytkownika i hasło Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów. Rozwiązanie musi obsługiwać monitorowanie hostów i serwerów w sieci wewnętrznej, identyfikując nazwę, system operacyjny, przeglądarkę, typ i rejestr statystyk zagrożeń sieciowych Oferowany zestaw urządzeń musi pochodzić o jednego producenta i być w pełni kompatybilny Oferowany zestaw urządzeń musi posiadać aplikację mobilną pozwalającą na monitoring pracy urządzeń i analizę zdarzeń
Logowanie i raportowanie	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. Raport można wyeksportować co najmniej w formacie PDF i/lub wysłać na adres e-mail lub FTP. Rozwiązanie powinno obsługiwać ustawianie alarmów dotyczących wykorzystania procesora, wykorzystania pamięci, wykorzystania miejsca na dysku, nowych połączeń itp. Rozwiązanie powinno obsługiwać wysyłanie alarmów przez e-mail, SMS. Alerty powinny być generowane na podstawie przepustowości aplikacji i nowych połączeń. Logi powinny być możliwe do eksportu za pośrednictwem Syslog lub poczty e-mail i zawierać minimum logi zdarzeń, sieci, zagrożenia, konfigurację i sesje Wstępnie zdefiniowane zadania raportowania Rozwiązanie powinno mieć scentralizowane monitorowanie wielu urządzeń, w tym procesora, pamięci, ruchu, sesji, aplikacji, użytkowników, zagrożeń itp. za pośrednictwem aplikacji mobilnej z danymi z ostatnich 7 dni. Rozwiązanie musi wspierać restAPI
Gwarancja	<p>Dostawa musi zawierać również:</p> <ul style="list-style-type: none"> 48-miesięczną gwarancję producenta na dostarczone elementy systemu Licencje na wszystkie funkcje bezpieczeństwa producentów na do 30.06.2026 (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C)

Parametr	Opis
	<ul style="list-style-type: none">• Wsparcie techniczne dystrybutora rozwiązań w języku polskim świadczone przez certyfikowanych inżynierów przez producenta na poziomie profesjonal• Szkolenie dla Administratorów z konfiguracji oferowanego rozwiązania przeprowadzone przez dystrybutora oferowanego rozwiązania w języku polskim• Oferta, wdrożenie oraz wsparcie musi być realizowane przez autoryzowanego partnera

2.1.1. Wymagania ogólne w zakresie dostawy sprzętu

Opis
Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nienoszący oznak użytkowania
Dostarczony sprzęt musi być fabrycznie nowy (tzn. wyprodukowane nie wcześniej, niż na 12 miesięcy przed ich dostarczeniem), musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu.
Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych, pochodzących z programów wyprzedażowych lub refabrykowanych. Urządzenia nie mogą znajdować się na liście end-of-sale, end-of-support producenta.
Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp. Niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów, jak kable DAC
Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V. Wymagane jest dostarczenie odpowiedniej ilości kabli zasilających z wtyczką europejską (typ C)
Dostarczony sprzęt musi zostać wdrożony przez inżyniera posiadającego certyfikat producenta sprzętu, który podlega dostawie.

2.2. Urządzenie typu Firewall UTM z oprogramowaniem SSL VPN 1 szt.

Urządzenie, o którym mowa dalej zwane systemem, urządzeniem, rozwiązaniem wraz z oprogramowaniem komercyjnym musi spełniać poniższe wymogi.

Parametr	Opis
Elementy systemu bezpieczeństwa	<ul style="list-style-type: none"> • Urządzenie musi mieć możliwość jednoczesnej pracy w trybie: <ul style="list-style-type: none"> A. Routera (warstwa trzecia) B. Switcha (warstwa druga) C. TAP • Możliwość stworzenia minimum 128 wirtualnych interfejsów zdefiniowanych jako VLAN w oparciu o standard 802.1Q. • W zakresie Firewall, obsługa nie mniej niż 2 200 000 jednoczesnych połączeń i 130 000 nowych połączeń na sekundę. • System realizujący funkcję Firewall musi być wyposażony we wbudowany dysk o minimalnej pojemności 8 GB do celów logowania i raportowania. • Możliwość rozszerzenia pamięci o co najmniej 1.92 TB poprzez dodatkowy dysk SSD, bez otwierania obudowy urządzenia • System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu. • System musi mieć możliwość włączenia min 1 systemu wirtualnego bez dodatkowej licencji i możliwość włączenia do

Parametr	Opis
	<p>minimum 5 systemów wirtualnych poprzez dokupienie dodatkowej licencji w przyszłości</p> <ul style="list-style-type: none"> Systemy wirtualne muszą obsługiwać QoS System pełniący funkcję zapory musi posiadać co najmniej: <ul style="list-style-type: none"> A. 8 interfejsów typu Gigabit Ethernet , w tym co najmniej jedną parę bypass B. 8 interfejsy typu SFP C. 2 interfejsy typu SFP+ / SFP D. 2 porty USB 3.0 z przodu urządzenia E. 1 port konsolowy RS232 lub Ethernet F. 1 dedykowany port Gigabit Ethernet przeznaczony do zarządzania System musi posiadać zewnętrzny przycisk, pozwalając na reset urządzenia do ustawień fabrycznych, bez konieczności logowania się do urządzenia
Funkcjonalności	<ul style="list-style-type: none"> Kontrola dostępu — zaporą sieciową Stateful Inspection Ochrona przed wirusami - komercyjny antywirus Poufność danych - IPSec VPN oraz SSL VPN Kontrola witryn sieci Web — filtr URL Kontrola zawartości poczty - antyspam dla protokołów SMTP oraz POP3 Kontrola przepustowości i ruchu – QoS Kontrola aplikacji i rozpoznawanie ruchu P2P (video, gry itp.) Reputacja IP Sandbox Moduł DLP API – możliwość wgrywania i czytania informacji interfejsem Rest API
Wydajność systemu	<ul style="list-style-type: none"> Wydajność Firewall: minimum 10.0 Gb/s dla pakietów o rozmiarze 1518 bajtów Wydajność NGFW (Kontrola Aplikacji, IPS): minimum 4.0 Gb/s Wydajność modułu IPS: minimum 8.0 Gb/s Wydajność AV: minimum 4.5 Gb/s Wydajność w trybie UTM (Kontrola Aplikacji, IPS, AV, URL): minimum 2.5 Gb/s.
Routing i Switching	<ul style="list-style-type: none"> System musi mieć możliwość zdefiniowania wielu Wirtualnych Switchy Wirtualne Switchy muszą obsługiwać tryb Virtual Wire System musi mieć możliwość zdefiniowania wielu Wirtualnych Routerów Rozwiązanie musi zapewniać obsługę co najmniej poniższych typów routingu: <ul style="list-style-type: none"> A. Routing Statyczny: <ol style="list-style-type: none"> 1. Destination routing

Parametr	Opis
	<ol style="list-style-type: none"> 2. Source routing 3. Policy Based routing <p>B. Routing dynamiczny:</p> <ol style="list-style-type: none"> 4. RIP 5. OSPF (w tym OSPF v3) 6. BGP 7. PIM (w tym PIMv6) <ul style="list-style-type: none"> • Zasady routingu pozwalają wybrać jako next-hop co najmniej: <ol style="list-style-type: none"> 1. Gateway 2. Interfejs 3. Inny Wirtualny Router • System musi umożliwiać wysyłanie kopii ruchu sieciowego na zdefiniowany przez administratora interfejs (Port Mirroring)
Wydzielanie stref bezpieczeństwa:	<ul style="list-style-type: none"> • System ma możliwość tworzenia osobnych stref bezpieczeństwa Firewall, osobno dla każdego z możliwych trybów pracy, np. <ol style="list-style-type: none"> 1. MGMT, LAN, WAN, DMZ dla trybu Routera 2. L2-LAN, L2-BYPASS dla trybu Switcha 3. TAP1, TAP2 dla trybu TAP • Strefa bezpieczeństwa pozwala na zdefiniowane jej ogólnych parametrów pracy, minimum: <ol style="list-style-type: none"> 1. Określenia jej typu 2. Określenie przynależności (Wirtualny Switch/Router) 3. Przypisanie odpowiednich interfejsów 4. Przypisanie wstępnych reguł i profilu bezpieczeństwa, niezależnych od później definiowanych polityk bezpieczeństwa (np. Strefa WAN zawsze będzie dokonywać inspekcji ruchu przychodzącego modułem IPS) • System ma możliwość zdefiniowania co najmniej 256 stref bezpieczeństwa
Polityka bezpieczeństwa systemu	<ul style="list-style-type: none"> • Polityka bezpieczeństwa systemu bezpieczeństwa musi uwzględniać minimum adresy IP, interfejsy lub strefy bezpieczeństwa, porty, protokoły, aplikacje, użytkowników, reakcje bezpieczeństwa, rejestrowanie zdarzeń, harmonogram • Możliwość zbudowania minimum 12000 polityk bezpieczeństwa • System musi posiadać funkcjonalność asystenta polityk, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego • System musi być w stanie zbudować agregowane polityki • Polityki bezpieczeństwa muszą posiadać licznik hitów, pozwalający szybko określić czy ruch przechodzi przez daną politykę

Parametr	Opis
	<ul style="list-style-type: none"> Polityki bezpieczeństwa muszą posiadać możliwość podglądu sesji przechodzących przez daną politykę System pozwala na łatwą zmianę pozycji polityki bezpieczeństwa na liście, dając minimum opcje umieszczenia jej na początku listy polityk oraz umieszczenia jej na końcu listy polityk System musi dawać możliwość łatwej zmiany kolejności polityk bezpieczeństwa, poprzez mechanizm przesuwania, tzw. drag and drop Rozwiązanie musi umożliwiać kopiowanie polityk bezpieczeństwa. Skopiowaną politykę można wkleić co najmniej na początku lub na końcu listy polityk
Translacja adresów NAT	<ul style="list-style-type: none"> Polityki NAT muszą być odrębne od polityk bezpieczeństwa Polityka NAT musi uwzględniać minimum typ, strefy bezpieczeństwa, adresy źródłowe i docelowe, interfejsy, porty, rejestrowanie zdarzeń, harmonogram Tłumaczenie adresu NAT źródłowego i adresu NAT docelowego. Obsługa NAT46, NAT64, DNS64 Obsługa trybów One-to-one, multi-to-one, multiport-to-one Wsparcie dla Sticky-connections oraz trybu Round-robin Wsparcie dla STUN Polityki NAT muszą posiadać licznik hitów, pozwalający szybko określić czy ruch przechodzi przez daną politykę Polityki NAT muszą posiadać możliwość podglądu sesji przechodzących przez daną politykę System pozwala na łatwą zmianę pozycji polityki NAT na liście, dając minimum opcje umieszczenia jej na początku listy polityk oraz umieszczenia jej na końcu listy polityk System musi dawać możliwość łatwej zmiany kolejności polityk NAT, poprzez mechanizm przesuwania, tzw. drag and drop Rozwiązanie musi umożliwiać kopiowanie polityk NAT. Skopiowaną politykę można wkleić co najmniej na początku lub na końcu listy polityk
QoS i Traffic Shaping	<ul style="list-style-type: none"> Polityki QoS muszą być odrębne od polityk bezpieczeństwa Polityka QoS musi uwzględniać minimum strefy bezpieczeństwa, interfejsy, adresy źródłowe i docelowe, użytkownika, serwisy, aplikacje, kategorie URL, VLAN id oraz TOS Sterowanie kształtowaniem ruchu musi odbywać się odrębnie dla ruchu wychodzącego oraz ruchu przychodzącego Minimalne i maksymalne pasmo może być określone w Kilo/Mega/Gigabitach na sekundę lub jako procentową wartość szybkości interfejsu

Parametr	Opis
	<ul style="list-style-type: none"> Limitowanie pasma może odbywać się dla: <ol style="list-style-type: none"> 1. Źródłowego adresu IP 2. Docelowego adresu IP 3. Użytkownika Istnieje możliwość zarezerwowania pasma przez konkretną politykę Polityka pozwala na nadpisanie Priority (0-7) oraz TOS System musi być w stanie ograniczyć sesje nowo nawiązywane oraz jednocześnie na podstawie strefy bezpieczeństwa, źródłowego adresu IP, docelowego adresu IP, harmonogramu, protokołu, aplikacji, użytkownik System musi pozwalać na ustawienie maksymalnej sumarycznej ilości danych wysłanych i odebranych przez użytkownika, w opcji dziennej oraz miesięcznej
Równoważenie obciążenia	<ul style="list-style-type: none"> Obsługa redundantnego równoważenia obciążenia łączy WAN z wykrywaniem jakości łącza: <ol style="list-style-type: none"> 1. Monitorowanie stanu łącza poprzez aktywną metodę wykrywania dla określonej nazwy domeny lub adresu IP protokołem ICMP lub TCP 2. Monitorowanie stanu łącza poprzez pasywną metodę wykrywania, co najmniej Opóźnienia, Jitter, Utrata pakietów Obsługa redundantnych łączy WAN pozwala na przetączenie się na drugie łącze w przypadku zbyt dużej użycia łącza głównego oraz w przypadku gdy wykrywanie jakości łącza zwróci wartość problematyczną (np. zbyt wysokie opóźnienia) Obsługa redundantnych łączy WAN pozwala na działanie w trybach force (natychmiastowe przetączenie nowych połączeń na drugie łącze) lub graceful (połączenia będą zachowywane w cache, nowe połączenia zgodne z cache nie będą przetączane na drugie łącze) System pozwala na równoważenie obciążenia serwerów (Load Balancing) Load Balancing może być oparty o algorytmy weighted hashing, weighted least connection i weighted round-robin Load Balancing pozwala na kontrolę stanu serwerów w oparciu o <ol style="list-style-type: none"> 1. PING 2. Połączenie TCP 3. Połączenie UDP Load Balancing pozwala na monitorowanie i limitowanie sesji oraz daje możliwość podtrzymania sesji
SSL Proxy i deszyfrowanie ruchu	<ul style="list-style-type: none"> System musi mieć możliwość analizy ruchu szyfrowanego protokołem SSL

Parametr	Opis
	<ul style="list-style-type: none"> Inspekcja może odbywać się w obu kierunkach ruchu, tzw. Client Inspection oraz Server Inspection (ruch użytkowników do Internetu oraz ruchu użytkowników do naszych serwerów) System musi wspierać deszyfrowanie co najmniej protokołów: HTTPS, POP3S, SMTPS, IMAPS, RDPS, FTPS System pozwala na wybranie co najmniej ośmiu kategorii URL, dla których deszyfracja ruchu nie będzie się odbywać (np. Bankowość, zdrowie) System musi wspierać co najmniej wersję TLS: 1.0, 1.1, 1.2, 1.3, z możliwością określenia najniższego oraz najwyższego wspieranego standardu TLS System daje możliwość blokady oraz zrobienia wyjątku dla połączenia w przypadku gdy: <ol style="list-style-type: none"> Wykryta jest niewspierana wersja TLS Wykryty jest niewspierany algorytm szyfrujący Pojawił się błąd przy deszyfracji Certyfikat serwera wygaś System umożliwia wybranie dowolnego certyfikatu (również własnego) za pomocą którego ruch będzie z powrotem szyfrowany System umożliwia pobranie certyfikatu którym ruch będzie ponownie szyfrowany, w celu importu go na stacje robocze by uniknąć błędów w przeglądarkach Rozwiązanie daje możliwość wyświetlenia użytkownikowi informacji o rozszywaniu ruchu, wraz z opcją pobrania niezbędnego certyfikatu potrzebnego do poprawnego działania przeglądarek
Funkcjonalności VPN:	<ul style="list-style-type: none"> System musi wspierać co najmniej poniższe metody połączeń VPN: <ul style="list-style-type: none"> IPSec VPN ze wsparciem dla IKEv1 oraz IKEv2 SSL VPN L2TP VPN GRE VPN VXLAN Wydajność IPSec VPN: minimum 5.0 Gb/s Tworzenie połączeń lokalizacja-lokalizacja i oraz klient-lokalizacja System musi pozwalać na jednoczesne zestawienie 6000 tuneli IPSec Producent oferowanego rozwiązania VPN musi zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem. Monitorowanie stanu tuneli VPN i utrzymywanie ich aktywności Praca w topologiach Hub and Spoke oraz Mesh

Parametr	Opis
	<ul style="list-style-type: none"> • Obsługa PnPVPN (Plug and Play VPN) • System musi wspierać mechanizmy : IPsec NAT Traversal, DPD, Replay Detection, XAuth, DHCP over IPsec • Wsparcie grup DH dla IKEv1: 1,2,5,19,20,21,24 • Wsparcie grup DH dla IKEv2: 1,2,5,14,15,16,18,19,20,21,24 • Wsparcie dla algorytmów Hashujących: MD5, SHA, SHA256, SHA384, SHA512 • Wsparcie dla algorytmów Szyfrujących: DES, 3DES, AES, AES192, AES256 • Wsparcia dla protokołów ESP oraz AH • Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance) co najmniej w zakresie: <ul style="list-style-type: none"> A. Wersji systemu operacyjnego B. Zaaplikowanych patchy C. Ustawień internetowych D. Zainstalowanego oprogramowania antywirusowego E. Włączonej zapory sieciowej F. Walidacji kluczy rejestru G. Walidacji istnienia plików H. Walidacji uruchomionych procesów I. Walidacji uruchomionych lub zainstalowanych serwisów • Możliwość jednoczesnego uwierzytelnienia co najmniej 4000 użytkowników VPN • Możliwość rozszerzania ilości użytkowników VPN odpowiednią licencją
Uwierzytelnianie użytkownika	<ul style="list-style-type: none"> • System bezpieczeństwa musi być w stanie przeprowadzić uwierzytelnianie tożsamości użytkownika z nie mniej niż: <ul style="list-style-type: none"> A. Statyczne hasła i definicje użytkowników przechowywane w lokalnej bazie danych systemu B. Statyczne hasła i definicje użytkowników przechowywane w bazach danych zgodnych z LDAP C. Statyczne hasła i definicje użytkowników przechowywane w Active Directory D. Hasła dynamiczne (RADIUS, TACACS+) oparte o zewnętrzne bazy danych E. Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA F. Serwer korzystający z OAuth 2.0 • System musi umożliwiać budowę architektury uwierzytelniania pojedynczego logowania (SSO) w środowisku Active Directory bez użycia agentów • Wsparcie dla usług terminalowych

Parametr	Opis
	<ul style="list-style-type: none"> • Uwierzytelnianie użytkownika przez panel Web przed dostępem do Internetu • Obsługa dwuskładnikowego uwierzytelniania: SMSy, certyfikaty i tokeny • System daje możliwość statycznego przypisywania użytkowników do adresów IP oraz adresów MAC • System musi mieć możliwość rozbudowy o moduł ZTNA, w celu uwierzytelniania użytkowników bazując na regułach i zasadach zdefiniowanych przed administratorem
Kontrola aplikacji	<ul style="list-style-type: none"> • Kontrola aplikacji musi być w stanie kontrolować ruch w oparciu o głęboką analizę pakietów, a nie tylko w oparciu o wartości portów TCP/UDP • Baza danych aplikacji musi zawierać ponad 6000 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka • Aplikacje muszą być pogrupowane wstępnie według kategorii (np. Biznesowe, Wideo, Gry) • Administrator ma możliwość dodawania swoich własnych aplikacji z poziomu konsoli web, bez konieczności kontaktu z producentem • Administrator ma możliwość dodawania swoich własnych kategorii aplikacji z poziomu konsoli web, bez konieczności kontaktu z producentem
Ochrona antywirusowa	<ul style="list-style-type: none"> • Silnik antywirusowy musi być oparty na przepływie tzw. flow-based • Silnik AV musi umożliwiać skanowanie co najmniej protokołów HTTP, SMTP, POP3, IMAP, FTP, SMB (w tym ich szyfrowanych odpowiedników po wcześniejszej deszyfracji) • Możliwość ręcznego dodawania oraz usuwania sygnatur MD5 do bazy danych AV • Możliwość ręcznego dodawania wyjątków w postaci sygnatur MD5 oraz URL • System musi obsługiwać wykrywanie wirusów w plikach skompresowanych, takich jak RAR, ZIP, GZIP, BZIP2, TAR, a także wykrywać wielowarstwowe pliki skompresowane dla nie mniej niż 5 warstw dekompresji
Ochrona IPS	<ul style="list-style-type: none"> • Moduł może działać w trybie detekcji (IDS) oraz w trybie ochrony (IPS) • Ochrona IPS musi opierać się przynajmniej na analizie protokołu i sygnatury. • Baza danych wykrytych ataków musi zawierać co najmniej 16000 sygnatur. Dodatkowo moduł musi być w stanie wykrywać anomalie protokołów i ruchu, które stanowią podstawową ochronę przed atakami DoS i DDoS.

Parametr	Opis
	<ul style="list-style-type: none"> • Moduł musi posiadać funkcjonalność zapobiegania atakom na serwery web, w tym przynajmniej: SQL injection, XSS, Hotlinking, HTTP Flood, Skany plików • System daje możliwość budowania własnych niestandardowych reguł IPS z poziomu interfejsu web, bez konieczności kontaktu z producentem • System ma możliwość wykrywania słabych haseł (ilość znaków mniejsza niż X, hasło takie jak login, znaki typu ciągi: np. abcdefgh) oraz haseł zdefiniowanych przez administratora, co najmniej w protokołach POP3, IMAP, SMTP, FTP, TELNET oraz HTTP (w tym w formularzach) • Moduł daje możliwość dodania wyjątków, bazując na adresie źródłowym, adresie docelowym oraz sygnaturze, którą chcemy wykluczyć
Obrona przed atakami sieciowymi	<ul style="list-style-type: none"> • Ochrona przed nieprawidłowym działaniem i anomaliami protokołów • Anti-DoS/DDoS, zawierający ochronę przed ICMP flood, SYN flood, UDP flood, DNS reply flood, DNS query flood, TCP fragment, ICMP fragment itp. • Wsparcie dla IPv4 i IPv6 dla ochrony przed DNS query flood i DNS reply flood • System musi zapewniać ochronę przed ARP Spoofingiem • System musi zapewniać ochronę przed skanowaniami portów oraz adresów • System musi zapewniać ochronę przed atakami typu Ping of Death, Fragmentacją IP czy też wykrywać nietypowo duże pakiety ICMP • System umożliwia zdefiniowanie białej lista docelowych/źródłowych adresów IP • System daje możliwość inteligentnego dostosowania parametrów ochrony ruchu, poprzez obserwację ruchu sieciowego organizacji przed zadany okres czasu. Dostosowanie parametrów może nastąpić automatycznie lub może być zatwierdzone przed administratora systemu
Ochrona antyspam	<ul style="list-style-type: none"> • Rozwiązanie musi zapewniać ochronę przed spamem w czasie rzeczywistym • Wspieranymi protokołami są minimum SMTP, SMTPS, POP3, POP3S • Skanowanie antyspamowe musi odbywać się w ruchu w obu kierunkach • Moduł musi rozróżniać różny typ spamu, w tym między innymi: Potwierdzony, Podejrzany, Masowe wiadomości • Musi istnieć możliwość dodawania wyjątków w zakresie skanowania antyspamowego, minimum białych list domen

Parametr	Opis
	oraz pojedynczych adresów email a także czarnych list domen oraz pojedynczych adresów email
Reputacja IP	<ul style="list-style-type: none"> • Identyfikacja i filtrowanie ruchu z ryzykownych adresów IP, takich jak hosty botnet, spamerzy, węzły Tor, podejrzan hosty i adresy IP atakujące metodą brute force • Logowanie, odrzucanie pakietów lub blokowanie dla różnych rodzajów ryzykownego ruchu IP
Zapobieganie botnetom	<ul style="list-style-type: none"> • Wykrywanie intranetowych hostów botnetu, monitorując połączenia C&C i blokując dalsze zaawansowanych zagrożenia takie jak przyłączenie do sieci botnet czy ataki ransomware • Wykrywanie połączeń co najmniej w protokołach TCP, HTTP oraz DNS • Wsparcie dla DNS sinkholing dostarczanego przez producenta • System daje możliwość ustawienia własnego serwera dla DNS sinkholeing • Możliwość wykrywania tunelowania DNS • Możliwość wykrywania i blokowanie DGA • Wykrywanie co najmniej poniższych typów połączeń: <ul style="list-style-type: none"> A. APT B. Miner C. CnC D. Trojan E. Ransomware F. Malware G. Phishing
Filtr adresów URL	<ul style="list-style-type: none"> • Baza filtrów URL pogrupowana w co najmniej 64 kategorie tematyczne. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków z poziomu konsoli web bez konieczności kontaktu z producentem • Możliwość zdefiniowania własnej bazy kategorii URL • System musi posiadać kategorie związane z bezpieczeństwem, takie jak Phishing, Malware, Spam, Botnety, P2P • Możliwość blokowania stron nieskategoryzowanych • Obsługa i wymuszanie trybu Safe Search • Możliwość blokowania pojedynczych adresów URL, bez konieczności tworzenia nowej kategorii • Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne lub słowa • Możliwość dostosowania strony ostrzeżenia/blokowania
Sandbox	<ul style="list-style-type: none"> • System daje możliwość emulowania oprogramowania w wirtualnym środowisku opartym na architekturze chmury w celu wykrywania nieznanych zagrożeń

Parametr	Opis
	<ul style="list-style-type: none"> • Obsługa minimum protokołów HTTP, POP3, IMAP, SMTP, FTP i SMB (w tym ich szyfrowanych odpowiedników po wcześniejszej deszyfracji) • Obsługa co najmniej typów plików : PE, ZIP, RAR, Office, PDF, APK, JAR, SWF, ELF a także skryptów: js, vbs, wsf ,hta, chm, pif, psl, bat • System daje możliwość dostosowania maksymalnej wielkości poszczególnych plików przesyłanych do analizy. • System daje możliwość dodawania wykrytych zagrożeń do białej listy
Ochrona danych DLP	<ul style="list-style-type: none"> • System ma możliwość kontroli przesyłanych plików poprzez protokoły: HTTP-POST, HTTP-GET, FTP, SMTP, POP3, IMAP, SMB (w tym ich szyfrowanych odpowiedników po wcześniejszej deszyfracji) • System ma możliwość blokady lub logowania przesyłanego pliku, bazując na jego parametrach, nie mniej niż na jego nazwie, minimalnej wielkości oraz typie pliku
Wysoka dostępność	<ul style="list-style-type: none"> • Rozwiązanie musi obsługiwać tryby Active/Active i Active/Passive bez konieczności dokupowania dodatkowej licencji • Rozwiązanie musi obsługiwać następujące opcje wdrażania HA: <ul style="list-style-type: none"> A. HA z agregacją linków B. Full mesh HA C. Geograficznie rozproszony HA
Raportowanie i przeglądanie logów	<ul style="list-style-type: none"> • Wbudowany w urządzenie bezpieczeństwa system raportowania i przeglądania logów nie może wymagać dodatkowej licencji na jego działanie • W zakresie dostarczonych funkcjonalności systemu raportowania i przeglądania logów oczekuje się nie mniej niż: <ul style="list-style-type: none"> A. Posiadanie predefiniowanych raportów dla ruchu internetowego, odwiedzanych adresów URL, zagrożeń sieciowych, uitylizowanych aplikacji B. System daje możliwość wygenerowania co najmniej 6 różnych raportów • System daje możliwość podglądania stanu ochrony w czasie rzeczywistym, oraz możliwość rozszerzenia widoku do co najmniej 30 dni • System musi zapewniać widoczność zagrożeń w czasie rzeczywistym, w tym pokazując minimum: <ul style="list-style-type: none"> A. Typ Zagrożenia B. Krytyczność zagrożenia C. Adres źródłowy ataku D. Adres docelowy ataku E. Geolokalizacje adresów IP

Parametr	Opis
	<p>F. Rezultat ataku (próba, udany)</p> <p>G. Datę oraz godzinę ataku</p> <ul style="list-style-type: none"> System musi posiadać predefiniowane ekrany, pozwalające ocenić na bieżąco status sieci, minimum pozwalające monitorować aktywność użytkowników, aktywność aplikacji, użycie interfejsów czy parametry pracy urządzenia
System logowania	<ul style="list-style-type: none"> System pozwala na lokalne gromadzenie logów dotyczących bezpieczeństwa, połączeń sieciowych, hitów w polityki bezpieczeństwa oraz polityki NAT oraz aktywności administratorów Wszystkie logi mają możliwość eksportu do zewnętrznych systemów logowania co najmniej za pomocą SYSLOG TCP, SYSLOG UDP oraz SYSLOG Secure-TCP Wszystkie logi mają możliwość zapisu na zewnętrznych nośnikach danych podpiętych do systemu za pomocą portu USB System ma również możliwość wysyłania logów na wskazane adresy E-Mail Wraz z systemem musi być zapewniony system długoterminowego logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy chmurowej, do której dostęp jest cały czas z dowolnego urządzenia oraz dedykowanej aplikacji mobilnej. Platforma może być hostowana przez producenta lub przez wykonawcę na okres trwania licencji.
Certyfikaty	<ul style="list-style-type: none"> Rozwiązanie musi posiadać certyfikat Common Criteria EAL4+ lub posiadać certyfikat ICSSA Labs dla funkcji Firewall Rozwiązanie musi być pozycjonowanym w raporcie Gartnera przez ostatnie 8 lat
Zarządzanie	<ul style="list-style-type: none"> Elementy systemu muszą mieć możliwość zarządzania lokalnie (HTTPS, SSH, TELNET, SNMP) oraz współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja między systemami bezpieczeństwa a platformami zarządzania musi odbywać się za pomocą protokołów szyfrowanych. Zarządzanie urządzeniem i konfiguracja musi odbywać się za pośrednictwem WebUI (HTTP lub HTTPS) bez instalowania oddzielnego oprogramowania, takiego jak dedykowana konsola Musi istnieć możliwość wyłączenia niebezpiecznych protokołów zarządzania takich jak HTTP czy TELNET Zarządzanie urządzeniem może odbywać się za pomocą linii komend dostępnej przez SSH, TELNET oraz Port Konsolowy. Komendy dostępne muszą się pokrywać między tymi sposobami zarządzania.

Parametr	Opis
	<ul style="list-style-type: none"> System musi posiadać możliwość uruchomienia lub otworzenia okna linii komend bezpośrednio z WebUI System musi posiadać panel Ulubione(Favorites), do którego można podpinąć poszczególne zakładki systemu, w celu uzyskania do nich szybszego dostępu w przyszłości System musi posiadać panel diagnostyczny, pozwalający na minimum: <ul style="list-style-type: none"> A. Uruchomienie poleceń DNS Query, Ping, Traceroute B. Uruchomienie zrzutu pakietów wedle ustalonych zasad C. Możliwość wgrania lub stworzenia pakietu, i przepuszczenia go przez system w celu sprawdzenia poprawności konfiguracji, działania polityk oraz mechanizmów ochrony System musi dawać możliwość selektywnego włączenia i wyłączenia zarządzania na poszczególnych interfejsach System musi mieć możliwość zdefiniowania adresów IP oraz adresów MAC, z których zarządzanie systemem będzie możliwe.
Gwarancja	<ul style="list-style-type: none"> 48-miesięczną gwarancję producenta na dostarczone elementy systemu Licencje na wszystkie funkcje bezpieczeństwa mają zostać dostarczone w ramach oferowanej gwarancji (IPS, AV, AS, QoS, Sandbox, URL, IP Reputation, Botnet C&C, DLP) Wsparcie techniczne dystrybutora rozwiązań w języku polskim świadczone przez certyfikowanych inżynierów przez producenta na poziomie professional Szkolenie dla Administratorów z konfiguracji oferowanego rozwiązania przeprowadzone przez dystrybutora oferowanego rozwiązania w języku polskim. Oferta, wdrożenie oraz wsparcie muszą być realizowane przez autoryzowanego partnera
Wdrożenie	<p>Wykonawca powinien wykonać następujące czynności:</p> <ul style="list-style-type: none"> Konfiguracja podstawowa (adresacja IP, dostęp administracyjny) Konfiguracja stref bezpieczeństwa (LAN, WAN, DMZ) Definicja i wdrożenie polityk firewall (reguły dostępu) Włączenie inspekcji aplikacyjnej (Layer 7) Konfiguracja IPS/IDS (Intrusion Prevention/Detection System) Wdrożenie filtrowania URL i treści Konfiguracja ochrony przed malware Włączenie kontroli aplikacji (Application Control) Konfiguracja VPN (IPSec/SSL) dla zdalnych użytkowników

Parametr	Opis
	<ul style="list-style-type: none"> Wdrożenie uwierzytelniania użytkowników (LDAP, RADIUS, MFA) Konfiguracja alertów i raportów bezpieczeństwa Testy reguł i scenariuszy awaryjnych Dokumentacja konfiguracji i polityk bezpieczeństwa Przygotowanie planu aktualizacji i kopii zapasowych

2.3. Zakup oprogramowania na potrzeby SSL/VPN

Wykonawca winien dostarczyć oprogramowanie spełniające wymagania opisane poniżej.

Lp.	Wymaganie	Opis szczegółowy
1	Moduł SSL VPN ZTNA z testowaniem zgodności hosta	Sprawdza: <ol style="list-style-type: none"> 1. Wersję systemu operacyjnego 2. Zaaplikowane patche 3. Włączony Windows Update 4. Ustawienia internetowe 5. Zainstalowany AV 6. Włączona zaporę sieciową 7. Hostname 8. Adres MAC 9. Klucze rejestru 10. Istnienie plików 11. Uruchomione procesy 12. Uruchomione/zainstalowane serwisy
2	Nadawanie tagów hostom	Możliwość przypisywania poziomów zaufania na podstawie spełnionych wymagań
3	Lista aplikacji dla użytkownika	Po połączeniu z ZTNA użytkownik widzi listę dostępnych aplikacji
4	Granularne ustawienia dostępu	W oparciu o: <ol style="list-style-type: none"> 1. Użytkownika/grupę 2. Tag 3. Aplikacje 4. ACL MAC adresów 5. Harmonogram
5	Konfigurowalny port nasłuchu	Możliwość ustawienia dowolnego portu przez administratora
6	Funkcjonalność 2FA	Co najmniej: <ol style="list-style-type: none"> 1. SMS 2. Email 3. Certyfikat
7	Jednoczesne uwierzytelnienie	Minimum 50 użytkowników
8	Skalowalność licencji	Możliwość rozszerzenia liczby użytkowników przez dodatkową licencję
9	Licencje	Forma: dożywotnia (perpetual)

2.4.Przetącniki sieciowe 6 szt.

Parametr	Opis
Ogólne	<ul style="list-style-type: none"> Zamawiający wymaga, aby miał pełne prawa do korzystania z licencji i oprogramowania zainstalowanego w urządzeniach Zamawiający wymaga, aby dostarczane urządzenia, a także ich wyposażenie i akcesoria montażowe były fabrycznie nowe i na dzień składania ofert niewycofane przez producenta ze sprzedaży Zamawiający wymaga, aby dostarczane urządzenia, a także ich wyposażenie i akcesoria montażowe pochodziły z oficjalnego kanału dystrybucyjnego producenta urządzeń na rynek polski Zamawiający wymaga, aby dostarczony sprzęt był zarejestrowany na Urząd lub jednostkę nadrzędną w celu posiadania pełnych praw licencyjnych i gwarancyjnych Zamawiający wymaga, aby wszystkie dostarczane urządzenia posiadały cechy/atributy ich legalności, tj. oznaczenie producenta, modelu oraz numeru seryjnego urządzenia Zamawiający wymaga, aby Wykonawca przed dostawą (najpóźniej w dniu dostawy) dostarczył numery seryjne urządzeń celem weryfikacji źródła ich pochodzenia u producenta. W przypadku negatywnej weryfikacji, Zamawiający może odmówić przyjęcia urządzeń.
Obudowa	<ul style="list-style-type: none"> Wysokość 1 U. Możliwość montażu do szafy RACK Wymiary maksymalne: <ul style="list-style-type: none"> szerokość: 445 mm głębokość: 288 mm wysokość: 44 mm Praca w szerokim zakresie temperatur: -5oC – 50oC Obsługa standardu Energy Efficient Ethernet (IEEE 802.3az)
Porty	<ul style="list-style-type: none"> 48 portów 10/100/1000BaseT RJ-45, 4x10G SFP+ Port konsoli – USB typu C i RJ45 posiadają zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)
Funkcje	<ul style="list-style-type: none"> Możliwość stackowania przetącników – do 200 portów w stosie – z wykorzystaniem wbudowanych portów 10G oraz z zachowaniem funkcji cross-stack w tym Link Aggregation i port mirroring Możliwość uruchomienia funkcji serwera DHCP Obsługa routingu dynamicznego z wykorzystaniem protokołu RIPv2 umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN i RSPAN z możliwością konfiguracji do 4 sesji monitorujących

	<ul style="list-style-type: none"> • posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp. • Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
Zasilanie i chłodzenie	Urządzenie wyposażone jest w wbudowany zasilacz AC 230V
Wydajność	<ul style="list-style-type: none"> • Pamięć DRAM – 1GB • Pamięć Flash – 512MB • Wielkość bufora pakietów – 1.5MB • Obsługa: • 4000 aktywnych sieci VLAN • 16000 adresów MAC • 990 statycznych tras IPv4 • 128 interfejsów IP • Obsługa ramek Ethernet Jumbo 9000B • 2000 grup IGMP • 8 grup połączeń zagregowanych typu „port channel” • Ilość wpisów w listach kontroli dostępu Security ACL – 1000
Protokoły	<ul style="list-style-type: none"> • Obsługa protokołu SNTP • Obsługa IGMPv1/2/3 i MLDv1/2 Snooping, • Obsługa protokołu sFlow • Obsługa protokołu LLDP i LLDP-MED • Obsługa Q-in-Q oraz Selective Q-in-Q
Bezpieczeństwo	<p>Ciągłość pracy w sieci:</p> <ul style="list-style-type: none"> • IEEE 802.1w Rapid Spanning Tree • Per-VLAN Rapid Spanning Tree (PVRST+) • IEEE 802.1s Multi-Instance Spanning Tree • Obsługa 126 instancji protokołu STP <p>Bezpieczeństwo sieci:</p> <ul style="list-style-type: none"> • Wiele poziomów dostępu administracyjnego poprzez konsolę • Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN • Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X • Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC • Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X • Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard • Obsługa funkcji IPv6 RA Guard, ND Inspection, DHCPv6 Guard

	<ul style="list-style-type: none"> • Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+ • Obsługa Private VLAN z możliwością definicji portów promiscuous, isolated i community • Obsługa list kontroli dostępu (ACL) – możliwość filtracji ruchu w oparciu adresy MAC (source/destination), VLAN ID, adresy IPv4 lub IPv6, TCP/UDP source/destination port, 802.1p priority, TCP flag. Obsługa czasowych list ACL • Obsługa mechanizmów zapewniających bezpieczną pracę urządzenia w tym ochronę procesów: Executable Space Protection [X-Space], Address Space Layout Randomization [ASLR], Built-In Object Size Checking [BOSC] • Bezpieczny proces bootowania urządzenia • Suplikant 802.1X - przetącznik można skonfigurować tak, aby działał jako suplikant do innego przetącznika
Jakość usług w sieci	<ul style="list-style-type: none"> • Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi • Implementacja algorytmu Weighted Round-Robin (WRR) dla obsługi kolejek • Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority) • Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP • Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi • Kontrola sztormów dla ruchu broadcast/multicast/unicast • Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP • Optymalizacja ruchu iSCSI - mechanizm nadawania priorytetu ruchowi iSCSI w stosunku do innych typów ruchu
Zarządzanie	<ul style="list-style-type: none"> • Port konsoli – USB typu C i RJ45 • Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu uaktualnienia oprogramowania urządzenia • Obsługa protokołów SNMPv3, SSHv2, https, syslog, SCP

	<ul style="list-style-type: none"> • Aplikacja mobilna umożliwiająca łatwe zarządzania urządzeniami • Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki • Tekstowy plik konfiguracyjny – z możliwością edycji z pomocą edytora tekstu
Wdrożenie	<p>Wykonawca ma obowiązek wdrożyć po dostawie urządzenie co oznacza, że powinien je zainstalować i skonfigurować w sposób gwarantujący nie tylko poprawne działanie, ale jednocześnie podnoszący poziom bezpieczeństwa urzędu. Wykonawca w ramach wdrożenia jest zobowiązany do:</p> <ul style="list-style-type: none"> • Nadania adresów IP do zarządzania • Konfiguracji VLAN-ów • Konfiguracji trunków i portów access • Włączenia Spanning Tree Protocol (STP) • Konfiguracji 802.1X (uwierzytelnianie urządzeń) • Wdrożenia Port Security • Utworzenia Access Control Lists (ACL) • Wyłączenia nieużywanych portów • Konfiguracji SNMP, Syslog, NetFlow/sFlow • Synchronizacji czasu (NTP) • Backup konfiguracji (TFTP/SFTP) • Konfiguracja redundancji (LACP, VRRP/HSRP) • Testy wydajności i bezpieczeństwa

2.5. Rozwiązanie do Backup'u

Parametr	Opis
Zarządzanie i magazyny	<ul style="list-style-type: none"> Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2025 r. System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu. Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe: <ul style="list-style-type: none"> Obudowa rack rozmiar: 1U Procesor: min. 6 rdzeni, min. 12 wątków. Minimalna częstotliwość bazowa procesora 2.6GHz Pamięć RAM: 16GB DDR4 Przestrzeń dostępna na przechowywanie danych: Min. 14TB po RAID 5 Osobne dyski SSD M.2 NVMe działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego, Redundantne zasilanie, Interfejsy sieciowe: Min. 2szt. Ethernet 1Gb, Gwarancja NBD on-premise o czasie trwania analogicznym do trwania wsparcia technicznego dla oprogramowania. Produkt dostępny w polskiej wersji językowej. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe System zarządzania nie może być oparty o relacyjne bazy danych.

- Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
- Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
- Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
- Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.
- System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
- System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
- System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.
- Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
- Rozwiązanie zapewnia backup jednorzeczny - nawet w przypadku wymagania granularnego odtworzenia.
- System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych
- Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.

- System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
- System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
- Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
- Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.
- System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,
- Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
- Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.
- Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).
- System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.
- Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.

- Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych
- Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.
- Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
- Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.
- Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
- Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
- System musi pozwalać na automatyczne aktualizacje oprogramowania.
- System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
- System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia.
- System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.
- System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
- Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie danych.

- System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
- System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.
- Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
- W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.
- Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
- System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
- System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
- System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental,
- Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
- Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3 oraz dedykowana chmura producenta appliance'u

	<ul style="list-style-type: none"> • Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb,S3, nfs, iscsi, katalog lokalny • Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS). • Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniem zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu. • Możliwość generowania raportów dobowych w oparciu o harmonogram • Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter powinno być zlokalizowane na terenie Polski) • Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna) • Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP. • Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienie e-mail. (poziom definiowany indywidualnie dla każdego magazynu)
Wspierane systemy	<ul style="list-style-type: none"> • Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy: <ol style="list-style-type: none"> 1. Alpine 3.10+, 2. Debian: 9+, 3. Ubuntu: 16.04+, 4. Fedora: 29+, 5. CentOS: 7+, 6. RHEL: 6+,

	<ol style="list-style-type: none"> 7. openSUSE: 15+, 8. SUSE Enterprise Linux(SLES): 12 SP2+, 9. macOS: 10.13+, 10. Windows: 7, 8.1, 10(1607+), 11. Windows Server: 2008 R2+, <ul style="list-style-type: none"> • Środowisk wirtualnych: <ol style="list-style-type: none"> 1. Hyper-V 2016+, 2. VMware: 6.7+.
Środowiska fizyczne i bazy danych	<ul style="list-style-type: none"> • Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami. • Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń. • Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej. • Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption. • System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji. • System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego skalania danych. • System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux. • W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem. • Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze

	<p>lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.</p> <ul style="list-style-type: none"> • Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych. • Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V. • Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK). • Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych. • Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).
Środowiska wirtualne	<ul style="list-style-type: none"> • System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów. • System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowaniem zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych. • System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych. • Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner. • System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych. • Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform

	<p>(inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).</p> <ul style="list-style-type: none"> • System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere. • System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.
Aplikacje SaaS	<ul style="list-style-type: none"> • Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza. • Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji) • System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365. • System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi • System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe. • System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git. • System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium. • System musi umożliwiać zabezpieczenie środowisk Jira • System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.
Licencjonowanie i wsparcie techniczne	<ul style="list-style-type: none"> • Wszystkie linie supportu muszą być obsługiwane w języku polskim. • Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta. • Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.

		<ul style="list-style-type: none"> • Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów) • Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego. • W ramach dostawy rozwiązania, dostawca musi wyznaczyć dedykowanego opiekuna technicznego od strony producenta rozwiązania backupowego. • W ramach dokumentacji posprzedażowej Dostawca musi dostarczyć bezpośredni numer telefonu oraz adres e-mail do dedykowanego opiekuna technicznego od strony producenta rozwiązania backupowego. • Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych. • Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu. • Wsparcie techniczne producenta musi zostać dostarczone do min. 30.06.2026 miesięcy. • System powinien pozwalać na replikację do innych zasobów. • Licencje powinny umożliwiać replikację na własne zasoby.
Anty-ransomware i bezpieczeństwo	i	<ul style="list-style-type: none"> • System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików"). • System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System • System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty. • W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.

	<ul style="list-style-type: none"> System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczonym urządzeniu.
Szkolenie	<ul style="list-style-type: none"> Szkolenie musi zostać przeprowadzone w formie zdalnej w języku polskim. Szkolenie jest realizowane bezpośrednio przez producenta oferowanego systemu backupowego. Szkolenie musi zostać przeprowadzone przez dedykowanego inżyniera producenta systemu backupowego. Szkolenie musi zakończyć się imiennym certyfikatem dla administratorów uczestniczących w szkoleniu. Szkolenie musi trwać minimum 2 godziny.
Wdrożenie	<ul style="list-style-type: none"> Wdrożenie zdalne musi zostać realizowane bezpośrednio przez producenta oferowanego systemu backupowego. Wdrożenie musi zostać przeprowadzone przez dedykowanego inżyniera od producenta systemu backupowego. Wdrożenie musi zakończyć się dostarczeniem dokumentacji powdrożeniowej, przygotowanej przez dedykowanego inżyniera od producenta systemu backupowego. Zamawiający powinien móc skorzystać z przynajmniej 2h pomocy wdrożeniowej bezpośrednio świadczonej przez producenta rozwiązania. Wdrożenie powinno być zrealizowane tak, aby dostosować się do preferencji zamawiającego

2.6.Oprogramowanie antywirusowe z modułem ochrony prewencyjnej - 75 licencji

Parametr	Opis
Konsola zarządzająca	<ul style="list-style-type: none"> Konsola web administratora powinna znajdować się w chmurze producenta znajdującej się na terenie Unii Europejskiej i zapewniać możliwość pełnego zarządzania stacjami roboczymi/serwerami przez przeglądarkę Web, która ma dostęp do Internetu. Konsola web administratora musi posiadać możliwość wyboru języka polskiego

- Konsola web musi umożliwiać zarządzanie stacjami roboczymi oraz serwerami i urządzeniami mobilnymi poprzez tą samą konsolę zarządzającą.
- Konsola web musi posiadać możliwość tworzenia grup i polityk dla stacji.
- Administrator musi mieć możliwość przenoszenia licencji pomiędzy urządzeniami stacjonarnymi i odrębnie między urządzeniami mobilnymi
- Administrator musi mieć możliwość zarządzania kluczem licencyjnym z poziomu konsoli administracyjnej.
- Konsola web musi umożliwiać bezpieczne logowanie do konsoli zarządzającej po protokole HTTPS z certyfikatem.
- Konsola web musi umożliwiać dwuetapową autoryzację logowania na minimum 2 sposoby.
- Konsola web musi posiadać możliwość zablokowania dostępu do ustawień programu ochrony dla użytkowników na urządzeniach nieposiadających uprawnień administracyjnych.
- Konsola web musi posiadać funkcję, która uniemożliwia użytkownikowi komputera wyłączenie działania monitora antywirusowego i innych składników ochrony, jeżeli nie posiada uprawnień administratora.
- Konsola web musi posiadać narzędzie do wykonania instalacji oprogramowania na stacjach poprzez Active Directory, grupy robocze lub zakresy adresów sieciowych IP.
- Konsola web musi umożliwiać wykonanie instalacji oprogramowania firm trzecich zdalnie z konsoli na stacjach bezpośrednio z bezpiecznego repozytorium dostawcy rozwiązania antywirusowego.
- Konsola web musi mieć możliwość zalogowania się kilku administratorom jednocześnie.
- Konsola web powinna oferować predefiniowane domyślne ustawienia rekomendowanych polityk (ustawień) dla stacji końcowych.
- Konsola web umożliwia zmianę ustawień priorytetu skanowania.
- Konsola web musi mieć funkcję planowania zadań, w tym planowania terminów automatycznego skanowania.
- Konsola web umożliwia wysyłanie powiadomień o zdarzeniach na wskazany adres mailowy.
- Konsola web musi posiadać możliwość uruchamiania komputerów zdalnie (WakeOnLAN), uruchamiania ponownego oraz wyłączania urządzeń z systemem Windows.
- Konsola web musi umożliwiać synchronizację z Azure Active Directory.
- Konsola web musi obsługiwać moduł do odbierania zgłoszeń serwisowych od użytkowników bezpośrednio z aplikacji zainstalowanej na stacji klienckiej.
- Rozwiązanie musi posiadać dedykowaną aplikację lub stronę internetową do zgłoszeń serwisowych bez konieczności instalacji ochrony antywirusowej.

	<ul style="list-style-type: none"> • Konsola web musi posiadać zintegrowany moduł CRM z możliwością zaplanowania prac u użytkownika. • Konsola web musi posiadać moduł uruchamiania procedur (skrypty) zdefiniowanych przez producenta oraz przez użytkownika w języku Python lub JSON. • Oprogramowanie web musi zawierać zintegrowaną funkcjonalność menadżera aktualizacji (Patch Manager), który umożliwia zarządzanie pobieraniem aktualizacji (update'ów) systemu Windows, Java, Adobe i innych producentów trzecich. • Producent powinien posiadać własne bezpieczne i sprawdzone repozytorium aplikacji do celów aktualizacji oprogramowania firm trzecich minimum 50 producentów.
Zarządzanie użytkownikami i stacjami	<ul style="list-style-type: none"> • Rozwiązanie musi umożliwiać bezpośrednio z konsoli zarządzającej web uruchamianie procedur (skryptów) serwisowych na stacjach klienckich o minimalnych, następujących funkcjonalnościach: <ul style="list-style-type: none"> ○ Czyszczenie plików tymczasowych ○ Czyszczenie i sprawdzanie dysku ○ Usuwanie błędów dysku ○ Defragmentowanie dysku ○ Czyszczenie kolejki drukarki ○ Czyszczenie pamięci podręcznej DNS ○ Czyszczenie kosza ○ Sprawdzanie błędów na dysku twardym S.M.A.R.T. Check ○ Włączenie szyfrowania dysku funkcją Bitlocker dla systemu Windows • System powinien przyjmować zgłoszenia serwisowe bezpośrednio z agenta na stacji, pocztą email oraz po przez dedykowaną stronę dla działu serwisu. • System musi umożliwiać przydzielanie zgłoszenia serwisowego dla konkretnego administratora oraz powinien mieć zintegrowany system diagnozy stacji oraz możliwość podłączenia się poprzez zdalny pulpit. • Konsola web musi posiadać zintegrowany moduł umożliwiający zdalne połączenie z graficznym pulpitem zdalnym przez dedykowaną aplikację dla komputerów/serwerów znajdujących się w sieci LAN i poza nią bez potrzeby tworzenia tuneli VPN każdej stacji komputera/serwera/Windows. • Możliwość wyświetlania komunikatu przed połączeniem zdalnym pulpitem do użytkownika przez administratora w określonym przez niego czasie. • Możliwość wyświetlania komunikatu przed połączeniem zdalnym pulpitem do użytkownika przez administratora w celu odpytania go o zgodę na połączenie. • Konsola web musi mieć funkcję tworzenia raportów o stacjach w konsoli. • Konsola web musi mieć funkcję logów wykonywanych czynności przez administratorów konsoli.

Agent ochrony konsoli – oprogramowanie antywirusowe

- Program antywirusowy powinien mieć obsługę w języku polskim. Platforma powinna obsługiwać systemy operacyjne:

macOS:

- 10.14.x
- 10.15.x
- 11.x
- 12.x
- 13.x
- 14.x

MS Windows (stacje klienckie):

- Windows XP (SP3 or higher) x86
- Windows 7 SP1 x86
- Windows 7 SP1 x64
- Windows 8 x86
- Windows 8 x64
- Windows 8.1 x86
- Windows 8.1 x64
- Windows 10 x86
- Windows 10 x64
- Windows 11 x64

MS Windows (wersja serwerowa):

- Windows Server 2003 SP2
- Windows Server 2003 R2 SP2
- Windows Server 2008 SP2
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

LinuxOS z gwarantowaną kompatybilnością:

- Latest Ubuntu 16.x LTS x64 release version (with GUI)
- Latest Ubuntu 18.x LTS x64 release version (with GUI)
- Latest Ubuntu 19.x x64 release version (with GUI)
- Latest Ubuntu 20.x LTS x64 release version (with GUI)
- Latest Ubuntu 21.04 x64 release version (with GUI)
- Latest Debian 8.x x64 release version (with GUI)
- Latest Debian 9.x x64 release version (with GUI)
- Latest Debian 10.x x64 release version (with GUI)
- Latest Red Hat Enterprise Linux Server 7.x x64 release version (with GUI)
- Latest Red Hat Enterprise Linux Server 8.x x64 release version (with GUI)
- Latest CentOS 7.x x64 release version (with GUI)
- Latest CentOS 8.x x64 release version (with GUI)

- Rozwiązanie powinno działać na komputerach wyposażonych minimalnie w:
 - 512 MB dostępnej pamięci RAM
 - 1 GB miejsca na dysku twardym dla wersji 32-bitowej i 64-bitowej
- Instalacja oprogramowania musi być możliwa poprzez Active Directory, grupy robocze, poprzez sieć, pobranie paczki MSI i za pomocą dystrybucji przez pocztę e-mail.
- Oprogramowanie powinno mieć możliwość przeglądania obciążenia procesów na stacji i serwerze oraz zawartości dysków z poziomu konsoli web.
- Ochrona poczty - antywirus musi chronić stacje poprzez uruchamianie nieznanych oraz niebezpiecznych załączników w środowisku wirtualnym na stacji takim jak lokalna i automatyczna piaskownica (auto-sandbox).
- Oprogramowanie umożliwia funkcję chat między administratorem konsoli a stacjami roboczymi (windows)
- Program antywirusowy musi posiadać możliwość skanowania wybranych plików, folderów/katalogów (również skompresowanych), a także całych dysków (w tym sieciowych) czy partycji.
- Oprogramowanie umożliwia cykliczne zrzuty ekranu podpiętych do konsoli stacji.
- Oprogramowanie umożliwia w konsoli WEB na:
 1. Podgląd uruchomionych procesów na danej stacji oraz ich zamknięcie
 2. Przeglądanie plików stacji końcowej
 3. Podgląd uruchomionych usług oraz ich restart i zakończenie
 4. Wykonywanie poleceń CMD i Powershell w przeglądarce
 5. Podgląd systemowego dziennika zdarzeń
- Oprogramowanie umożliwia pełną wizualną personalizację aplikacji.
- Oprogramowanie umożliwia przypisanie aplikacji z repozytorium udostępnionego przez producenta
- Oprogramowanie umożliwia na rejestrowanie lokalne wszystkich zdarzeń z aplikacji oraz wysyłanie ich na zewnętrzny serwer SYSLOG
- Oprogramowanie umożliwia monitorowanie:
 - Monitorowanie wydajności pracy: CPU, RAM, sieci, dysku
 - Rozmiaru plików i folderów
 - Pojemności dysku
 - Aktywnych procesów
 - Podgląd dziennika zdarzeń systemu
 - Aktywnych połączeń sieciowych
 - Stron WWW
 - Zdarzeń aktualizacji systemu operacyjnego
- Program antywirusowy musi posiadać możliwość skanowania dowolnego zasobu podłączonego do stacji roboczej np.: dyski zewnętrzne, pamięci USB

- Program antywirusowy powinien posiadać filtering URL umożliwiający blokowanie konkretnych stron internetowych.
- Program antywirusowy musi posiadać moduł antywirusowy chroniący w czasie rzeczywistym.
- Program antywirusowy musi posiadać moduł sprawdzający reputację plików w chmurze.
- Program antywirusowy musi posiadać dwukierunkowy konfigurowalny z konsoli web firewall z możliwością tworzenia polityk globalnych i z podziałem na aplikacje.
- Program antywirusowy musi posiadać moduł HIPS (Host Intrusion Protection System – ochrona antywłamaniowa).
- Program antywirusowy musi posiadać moduł automatycznej piaskownicy (autosandbox), odizolowanego środowiska wirtualnego, w którym zasoby są emulowane dla obiektów w nim umieszczonych. Dodatkowo cały proces izolacji dzięki temu modułowi musi odbywać się lokalnie, na stacji roboczej. Całe środowisko wirtualne musi być odwzorowaniem 1:1 z systemem operacyjnym. Użytkownik powinien móc pracować w zwirtualizowanym środowisku, bez możliwości zapisu na stacji poza środowiskiem wirtualnym.
- Program antywirusowy musi posiadać możliwość uruchomienia dowolnego pliku/programu w automatycznej piaskownicy (auto-sandbox) na żądanie użytkownika (manualnie).
- Program antywirusowy musi umożliwiać użytkownikowi wysłanie podejrzanego obiektu do producenta oprogramowania antywirusowego w celu jego analizy. Funkcja ta powinna być dostępna z interfejsu programu antywirusowego.
- Podczas pracy komputera Program musi automatycznie skanować:
 - pliki uruchamiane, otwierane,
 - pliki kopiowane lub przenoszone,
 - pliki tworzone,
 - pliki pobierane z Internetu po protokole HTTP/HTTPS.
- W przypadku wykrycia wirusa program musi posiadać możliwość automatycznego poddawania kwarantannie podejrzanych obiektów oraz opcję przywrócenia z kwarantanny usuniętych obiektów.
- Program antywirusowy musi posiadać funkcję dodawania wyjątków do modułu antywirusowego, automatycznej piaskownicy (auto-sandbox) czy modułu HIPS.
- Program antywirusowy powinien posiadać dodatkowe narzędzie do skanowania systemu.
- Program antywirusowy musi posiadać dodatkowe narzędzie do analizowania bezpieczeństwa procesów.

- Program antywirusowy powinien mieć możliwość skanowania skompresowanych plików.
- Program antywirusowy musi być z możliwością zablokowania dostępu do zmiany ustawień programu hasłem administratora oraz hasłem skonfigurowanym w konsoli zarządzającej.
- Program antywirusowy powinien mieć możliwość importowania oraz eksportowania ustawień.
- Program antywirusowy powinien mieć możliwość tworzenia list zaufanych procesów.
- Program antywirusowy powinien mieć możliwość tworzenia list zaufanych plików.
- Program antywirusowy i konsola powinny umożliwiać tworzenie wyjątków ze skanowania folderów / plików.
- Program antywirusowy powinien umożliwiać konfigurację polityk (globalnych ustawień dla grup endpoint'ów) w celu szybkiej implementacji ustawień bezpieczeństwa dla wielu urządzeń.
- Program antywirusowy powinien umożliwiać zmianę ustawień priorytetu skanowania.
- Program antywirusowy powinien umożliwiać skanowanie pamięci komputera po uruchomieniu.
- Program antywirusowy posiada zintegrowaną funkcję skanowania i ochrony plików pod kątem danych wrażliwych (DLP).
- Program antywirusowy posiada zintegrowaną funkcję blokowania urządzeń zewnętrznych / przenośnych przed odczytem, edycją i zapisem plików w tym samym czasie.
- Program antywirusowy posiada zintegrowaną funkcję blokowania jedynie zapisu plików na urządzeniach zewnętrznych / przenośnych.
- Program antywirusowy powinien posiadać możliwość aktualizowania baz danych antywirusowych ręcznie, nawet jeśli komputer nie będzie miał dostępu do Internetu.
- Program antywirusowy musi posiadać zintegrowane środowisko, dzięki któremu możemy bezpiecznie działać w wirtualnym systemie nawet na zainfekowanej stacji. Środowisko to musi być odizolowane od reszty systemu operacyjnego i mieć możliwość uruchomienia takich sesji bez wprowadzonych wcześniejszych zmian przez użytkownika w tym narzędziu (czyste środowisko). Ma również pozwalać na bezpieczniejsze wykonywanie przelewów bankowych, bez obaw, że system operacyjny, na którym działa dany komputer nie został uprzednio zmodyfikowany i byłby w stanie zagrozić utracie np. danych logowania do kont bankowych.

	<ul style="list-style-type: none"> • Oprogramowanie powinno mieć możliwość przeglądania obciążenia procesów na stacji i serwerze oraz zawartości dysków z poziomu konsoli web. • Oprogramowanie umożliwia funkcję chat między administratorem konsoli a stacjami roboczymi (windows) • Oprogramowanie chroni przed nieupoważnionym rzutem obrazu z ekranu. • Oprogramowanie umożliwia analizę skryptu w programach pod kątem złośliwego oprogramowania przed ich uruchomieniem. • Oprogramowanie umożliwia na rejestrowanie dzienników zdarzeń oraz zapisywanie ich lokalnie i na zewnętrznym serwerze. • Oprogramowanie umożliwia personalizację wyglądu agenta ochrony. • Oprogramowanie umożliwia zastosowanie proxy do rozpropagowania aktualizacji wewnątrz sieci. • Oprogramowanie umożliwia procentową regulację zużycia zasobów procesora oraz nadania priorytetu. • Oprogramowanie umożliwia śledzenie bibliotek uruchomionych przez procesy oraz blokowanie nieznanych bibliotek.
Dodatkowe systemy bezpieczeństwa	<ul style="list-style-type: none"> • Konsola web musi posiadać możliwość śledzenia historii zagrożeń na wybranych komputerach. • Konsola web musi posiadać moduł zapobiegania wyciekowi danych DLP możliwością włączenia skanowania plików w wybranych lokalizacjach na komputerach pod kątem znajdujących się w nich danych wrażliwych przez zdefiniowane wzory z możliwością dodawania własnych reguł DLP oraz powinna umożliwiać sprawdzenia logów z tej czynności. • Konsola web zintegrowana z wszystkimi poprzednimi modułami i funkcjami musi umożliwić przeprowadzenia skanowania sieci firmowej (również za pomocą protokołu SNMP) w celu przeprowadzenia audytu urządzeń działających w tej sieci.
Moduł detekcji zagrożeń na urządzeniach końcowych	<ul style="list-style-type: none"> • Rozwiązanie zawiera w sobie moduł oparty na technologii typu "Endpoint Detection & Response", zwany dalej EDR. • Moduł EDR ma funkcję śledzenia zdarzeń systemowych i sieciowych urządzeń na których jest wdrożony. • Moduł EDR ma funkcję alertowania wybranych zdarzeń, typowanych na stanowiące potencjalne zagrożenie dla cyberbezpieczeństwa, zgodnie z przyjętą polityką. • Polityka bezpieczeństwa musi być edytowalna i mieć możliwość wprowadzania samodzielnie zdefiniowanych reguł. Nie jest dopuszczalne ograniczenie do reguł predefiniowanych przez producenta.

	<ul style="list-style-type: none"> Funkcja śledzenia zdarzeń musi mieć możliwość ich filtrowania względem co najmniej 10-ciu parametrów, w szczególności: <ul style="list-style-type: none"> a) urządzenia b) użytkownika c) podsystemu bezpieczeństwa d) techniki potencjalnego ataku. e) taktyki potencjalnego ataku. Moduł EDR musi mieć możliwość korelacji ewentualnych powiązań pomiędzy śledzonymi zdarzeniami i przedstawienia ich z użyciem sygnatur czasowych i/lub na osi czasu. Korelacja zdarzeń śledzonych przez EDR ma dotyczyć w szczególności: <ul style="list-style-type: none"> a) zmian w plikach b) zmian w rejestrze systemowym c) działających procesów i podprocesów d) dostępu do urządzeń zewnętrznych
Dostawa, gwarancja i usługa wdrożeniowa	<ul style="list-style-type: none"> Licencja na oprogramowanie ma mieć charakter subskrypcyjny i obowiązywać co najmniej do 30.06.2026 Dostawa musi zawierać również szkolenie dla Administratorów z konfiguracji oferowanego rozwiązania przeprowadzone przez dystrybutora oferowanego rozwiązania w języku polskim Oferta musi być złożona przez autoryzowanego partnera Wsparcie techniczne producenta powinno obowiązywać min. 24 miesiące. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie określonej przez Zamawiającego ilości hostów w obrębie wspieranych przez System środowisk: 75 stacji roboczych w tym min. 5 serwerów Windows Server. Zamawiający dopuszcza rozwiązanie równoważne różnych producentów zgodne z opisem przedmiotu zamówienia pod warunkiem iż będą one posiadać jedną centralną konsolę do zarządzania wszystkimi komponentami systemu oraz będą obsługiwane przez jedno centralne wsparcie techniczne w języku Polskim.