Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. **Przedmiotem umowy jest zakup i dostawa sprzętu komputerowego i oprogramowania wraz z usługą wdrożenia w ramach realizacji projektu „Cyberbezpieczny Samorząd" realizowanego przez Gminę Siechnice.**
   Niniejsze zamówienia ma na celu podniesienie standardów bezpieczeństwa informacji w Gminie Siechnice poprzez szereg inwestycji w infrastrukturę serwerową, narzędzia informatyczne oraz środki organizacyjne aby zapewnić cyberodporność infrastruktury. Zachowując ciągłość realizowania zadań publicznych, wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach teleinformatycznych.

L.p.	Grupa	Przedmiot zamówienia	Ilość / jednostka miary
1.	Zadanie 1	Serwer	1 kpl.
2.	Zadanie 1	Serwer do wykonywania kopii bezpieczeństwa	2 kpl.
3.	Zadanie 1	Oprogramowanie do wykonywania kopii bezpieczeństwa	1 szt.
4.	Zadanie 2	UTM wraz z serwisem	1 kpl.
5.	Zadanie 2	UTM wraz z serwisem	3 kpl.
6.	Zadanie 2	Klient VPN (Zero Trust Network Access)	50 szt.
7.	Zadanie 2	Analizer Logów	1 szt.
8.	Zadanie 2	System EDR, XDR zintegrowany z systemem antywirusowy	200 szt.
9.	Zadanie 2	System DLP	200 szt.
10.	Zadanie 2	System do zarzadzania czynnościami użytkowników i sprzętu	200 szt.
11.	Zadanie 2	Rozwiązanie do backupu maili sprzęt	1 kpl.
12.	Zadanie 2	Rozwiązanie do backupu maili	1 kpl.
13.	Zadanie 3	Opracowanie i wdrożenie dokumentacji SZBI oraz KRI Procedur zgodnej z normą 27001 w tym aktualizacja Polityk bezpieczeństwa: Utworzenie procedury obsługi incydentów, ciągłości Działania.	1 kpl.
14.	Zadanie 4	Szkolenia dla pracowników IT	3 kpl.
15.	Zadanie 4	Szkolenia pracowników w zakresie cyberbezpieczeństwa	160 kpl.
16.	Zadanie 4	Wdrożenia przy asyście inżynierów, opieka inżynieryjna na czas trwania projektu	1 kpl.

1) Serwer – 1 szt.

Nazwa	Minimalne wymagania
Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli) Możliwość wyposażenia serwera w zamykany, zdejmowany panel przedni chroniący przed nieuprawionym dostępem do dysków Możliwość wyposażenia serwera w czujniki otwarcia obudowy współpracującego z BIOS/UEFI. Zainstalowany moduł TPM 2.0.
Procesor	Zamontowane minimum dwa procesory 20-rdzeniowe, x86 - 64 bity, osiągający w testach PassMark – CPU Mark wynik nie gorszy niż 40533 punktów dla konfiguracji dwuprocesorowej. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.cpubenchmark.net w okresie od 15.09.2024 do dnia zakończenia składania ofert. Płyta główna wspierająca zastosowanie procesorów od 4 do 28 rdzeniowych, mocy do min. 205W i taktowaniu CPU do min. 3.6GHz.
Liczba procesorów	Min. 2 procesory
Pamięć operacyjna	640 GB RDIMM DDR4 2993 MT/s w modułach o pojemności 64GB każdy. Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację do minimum 3TB. Obsługa zabezpieczeń: Advanced ECC i Online Spare. Serwer z obsługą pamięci typu NVDIMM
Sloty rozszerzeń	8 aktywnych gniazda PCI-Express generacji 3, w tym min. 2 slot x16 (szybkość slotu – bus width) pełnej wysokości (full height).
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania 16 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5” i opcja rozbudowy/rekonfiguracji serwera o dodatkowe 8 dysków typu Hot Swap, SAS/SATA/SSD, 2,5” montowane z przodu obudowy. W przypadku braku opcji rozbudowy/rekonfiguracji o dodatkowe zatoki dyskowe, serwer standardowo wyposażony w minimum 24 zatok dyskowych SFF gotowych do instalacji dysków SAS/SATA/SSD 2,5”typu Hot Swap. Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 32GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera. Zainstalowane 8 dysków 3.84TB SAS12G SSD Read-intensive.
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60 oraz SAS Expander umożliwiający obsługę wszystkich dysków montowanych z przodu serwera przez jeden kontroler RAID.

	Serwer umożliwiający rozbudowę o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem bateryjnym. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie
Interfejsy sieciowe	Minimum 4 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń” z chipsetem Intel I350. Zainstalowane 4 karty 4x1GB RJ-45. Zainstalowane 2 karty 2x10GB SFP+ wraz z wkładkami 10GB SR. Zainstalowana 1 karta dwu-portowa FC16GB.
Karta graficzna	Zintegrowana karta graficzna
Porty	Minimum 5 x USB 3.0 (w tym 2 porty wewnętrzne) 1x VGA Wewnętrzny slot na kartę micro SD. Możliwość rozbudowy o: - dodatkowy port typu DisplayPort dostępny z przodu serwera - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1000W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Napęd	Możliwość instalacji wewnętrznego napędu DVD-ROM lub DVD-RW
Diagnostyka	Możliwość wyposażenia w elektroniczny panel diagnostyczny dostępny z przodu serwera pozwalający uzyskać informacje o stanie: procesora, pamięci, wentylatorów, kary sieciowej, zasilaczy, kartach rozszerzeń, temperaturze.
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia mininmalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI)

	- z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne
Wsparcie techniczne	Minimum 3-letnia gwarancja producenta w miejscu instalacji. Czas reakcji w miejscu instalacji to kolejny dzień roboczy. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera.
PRZEDMIOTOWE ŚRODKI DOWODOWE	Wymagane dołączenie do oferty oświadczenie producenta sprzętu potwierdzające, że serwis realizowany będzie bezpośrednio przez producenta oferowanego serwera.
System operacyjny	Wraz z serwerem należy dostarczyć Windows Serwer 2022 Datacenter na wszystkie fizyczne rdzenie procesorów oraz 200 szt. CAL-i per User i 40 szt. RDS CAL per User
PRZEDMIOTOWE ŚRODKI DOWODOWE	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Zamawiający wymaga dostarczenia wraz z ofertą oświadczenia producenta oferowanego serwera, potwierdzającego pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.

2) Serwer NAS z dyskami HDD – 2 szt.

Nazwa	Minimalne wymagania
Procesor	Procesor osiągający wynik min. 4 tysięcy punktów w teście PassMark.
Obudowa	Rack o wysokości maksymalnie 3U z szynami przesuwnymi w zestawie.
Pamięć RAM	Minimum 32GB DDR4 ECC UDIMM Możliwa rozbudowa do minimum 64GB (2 x 32GB).
Ilość obsługiwanych dysków	Minimum 16 dysków 3,5”/2,5” SATA 6 Gb/s o maksymalnej pojemności min. 22TB każdy.
Zainstalowane dyski	Minimum 8 dysków o pojemności 8TB każdy zgodnych z listą kompatybilności oferowanego serwera oraz charakteryzujące się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM, - pamięć cache: minimum 256MB, - pobór mocy podczas pracy: maksymalnie 8W, - gwarancja: minimum 60 miesięcy, - MTBF: minimum 2 miliony.
Interfejsy sieciowe	Minimum 2 porty 2,5GbE RJ-45, Obsługa VLAN i Jumbo Frame.

	Możliwość dołożenia karty z portami 10GbE (SFP+), 25GbE (SFP28) lub 16/32 Gb/s Fibre Channel.
Porty	Minimum 2 porty USB 3.2 Gen 1 typu A Minimum 2 porty USB 3.2 Gen 2 typu C
Porty PCIe	Minimum 2 gniazda PCIe Gen3 x4.
Wskaźniki LED	Stan serwera, LAN, USB, HDD 1–16
Obsługa RAID	RAID 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity, RAID 5, 6, 10 + dysk zapasowy.
Funkcje RAID	Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD.
Szyfrowanie	256-bitowe szyfrowanie AES folderów oraz szyfrowanie dysków zewnętrznych.
Wsparcie dla systemów operacyjnych	Apple Mac OS 10.10 lub nowszy Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux IBM AIX 7, Solaris 10 lub nowszy UNIX Microsoft Windows 7, 8, 10, 11 Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer WWW, Serwer plików, Manager plików przez WWW, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog,
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
Język GUI	Polski
Gwarancja i serwis	Minimum 24 miesięcy gwarancji NBD On-site świadczonej przez autoryzowany serwis producenta.
Waga	Maksymalnie 14 kg (bez dysków HDD).
Pobór mocy	Praca: maksymalnie 105 W
System plików	Dyski wewnętrzne - ZFS. Dyski zewnętrzne - EXT3, EXT4, NTFS, FAT32, HFS+.
Funkcje systemu plików	Liniowa deduplikacja, kompresja i kompakcja, Cache odczytu & ZIL
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Liczba kont użytkowników	Minimum 4096
Liczba grup	Minimum 512
Liczba udziałów	Minimum 512
Ilość połączeń (CIFS) z	Minimum 1800

maksymalnie rozbudowaną pamięcią RAM	
Max liczba migawek	Minimum 65535
Zasilanie	Redundantny zasilacz o mocy minimum 500W.
Wentylatory	Minimum 3 wentylatory o rozmiarze nie mniejszym niż 60mm x 60mm, 12VDC
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.

3) Oprogramowanie do wykonywania kopii bezpieczeństwa.

Oprogramowanie do kopii zapasowej hostów wirtualnych, serwerów fizycznych oraz komputerów klienckich, licencja stała, wieczysta, bezterminowa	
Wymagania	Licencja musi uprawniać Zamawiającego do zastosowania oprogramowania do kopii zapasowej 20 hostów wirtualizacji ESXI lub Hyper-V
Funkcjonalności systemu	- Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich - Program serwerowy kompatybilny z systemami: Microsoft Windows Windows 10; Windows 11; Microsoft Windows Server 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology - Program kliencki kompatybilny z systemami: Windows 10; Windows 11; Microsoft Windows Server 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology - Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików) - Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS) - Automatyczny backup przy wyłączaniu komputera - Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików - Backup całego systemu operacyjnego i zainstalowanych programów dla systemów z rodziny Windows - Backup baz danych i plików poczty w trybie online i offline - Kopie rotacyjne (wersjonowanie) - Zapis archiwów w otwartym formacie (ZIP 64-bit) - Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi - Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore) - Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej - Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych - Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO - Kompresja po stronie stacji roboczej - Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP, - Replikcacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (min. Windows) - Centralne sterowanie całym Systemem z jednego miejsca - Transparentna archiwizacja wykonywana w tle

	- Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN - Wysyłanie Alertów administracyjnych na e-mail, obsługa SMTPS -Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych - Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki - Automatyczna aktualizacja oprogramowania na komputerach zdalnych - Interfejs, instrukcja i pomoc techniczna w języku polskim - minimum dwuosobowa kontrola administracyjna

4) UTM – 1 szt.

Nazwa	Minimalne wymagania
Wymagania ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie:	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 18 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps.

	• 4 gniazdami SFP+ 10 Gbps. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie 2xAC.
Parametry wydajnościowe:	1. W zakresie Firewall'a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 280 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 26 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 12.6 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 12.5 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 4.8 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3.9 Gbps.
Funkcje Systemu Bezpieczeństwa:	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań

	DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

	• Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (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.
Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii

	URL.
Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System wstrzymuje dostarczenie pliku, dla którego jest realizowana analiza z wykorzystaniem systemu Sandbox, do czasu otrzymania werdyktu z systemu Sandbox. 9. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 10. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 11. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.

	8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

	• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów

	sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Testy wydajnościowe oraz funkcjonalne	1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox realizowana inline, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Security compliance (audyt konfiguracji i polityk urządzenia) na okres 18 miesięcy.
Wdrożenie	Wdrożenie musi być prowadzone przez jednego certyfikowanego inżyniera, posiadającego minimum 4 aktywne certyfikaty producenta oferowanego w postępowaniu rozwiązania UTM na poziomie: • Certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci(NS) • Certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej(PCS) • Certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa(SO) • Certyfikowany Specjalista w zakresie Dostępu Zero Trust(ZTA)
Gwarancja oraz wsparcie	System jest objęty serwisem gwarancyjnym producenta przez okres minimum 18 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Rozszerzone wsparcie serwisowe AHB/SOS	System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres minimum 18 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.
PRZEDMIOTOWE ŚRODKI DOWODOWE	Wymagania powinny być potwierdzone dokumentami: • Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego.
PRZEDMIOTOWE ŚRODKI DOWODOWE	1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do

	technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany 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. 2. Zamawiający wymaga, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

5) UTM – 3 szt.

Wymagania Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

	3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie:	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 5 portami Gigabit Ethernet RJ-45. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe:	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps. 5. 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 1 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.
Funkcje Systemu Bezpieczeństwa:	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

	11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	Polityki, Firewall 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
Połączenia VPN	• System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

	• Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. • System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (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.
Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System wstrzymuje dostarczenie pliku, dla którego jest realizowana analiza z wykorzystaniem systemu Sandbox, do czasu otrzymania werdyktu z systemu Sandbox. 9. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

	10. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 11. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

	4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Testy wydajnościowe oraz funkcjonalne	1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox realizowana inline, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Security compliance (audyt konfiguracji i polityk urządzenia) na okres minimum 18 miesięcy.

Wdrożenie	Wdrożenie musi być prowadzone przez jednego certyfikowanego inżyniera, posiadającego minimum 4 aktywne certyfikaty producenta oferowanego w postępowaniu rozwiązania UTM na poziomie: • Certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci(NS) • Certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej(PCS) • Certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa(SO) • Certyfikowany Specjalista w zakresie Dostępu Zero Trust(ZTA)
Gwarancja oraz wsparcie	1. System jest objęty serwisem gwarancyjnym producenta przez okres minimum 18 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Rozszerzone wsparcie serwisowe AHB/SOS	System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres minimum 18 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.
PRZEDMIOTOWE ŚRODKI DOWODOWE	Wymagania powinny być potwierdzone dokumentami: • Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego.
Opisy do wymagań ogólnych	1. Wymagane jest, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany 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. 2. Wymaga się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

6) VPN – 50 szt.

Zaawansowana ochrona stacji roboczych – rozbudowa obecnego systemu.	Przedmiotem postępowania jest rozbudowa istniejącego systemu bezpieczeństwa infrastruktury teleinformatycznej o elementy zabezpieczeń dla stacji roboczych wraz z mechanizmami centralnego zarządzania. Dostarczone rozwiązanie do ochrony stacji roboczych musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji.
System ochrony dla stacji roboczych wraz z systemem centralnego zarządzania.	Wykonawca dostarczy rozwiązanie do ochrony stacji roboczych wraz z mechanizmami centralnego zarządzania. Dostarczone rozwiązanie do ochrony stacji roboczych musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji.
Parametry systemu ochrony dla stacji roboczych.	1. Elementy systemu ochrony dla stacji roboczych powinny zapewniać następujące funkcje i mechanizmy: • Kontrola antywirusowa. • Funkcja analizy plików w zewnętrznym systemie Sandbox. • Opcja kwarantanny lokalnej plików przesłanych do Sandbox na czas analizy. • URL filtering w oparciu o kategorie stron z opcją definiowania wyjątków. • Kontrola aplikacji - w oparciu o wbudowany Firewall aplikacyjny. • Mechanizmy analizy podatności na stacji roboczej - pozwalające wykryć zagrożenia w systemie operacyjnym oraz zainstalowanych aplikacjach. • Mechanizmy szyfrowanych połączeń typu IPSec VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu. • Mechanizmy szyfrowanych połączeń typu SSL VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu. • Możliwość zastosowania certyfikatów cyfrowych w procesie uwierzytelnienia przy realizacji szyfrowanych połączeń. • Mechanizmy uwierzytelniania dwuskładnikowego • AntiExploit, • blokowanie dysków przenośnych typu USB, 2. Poszczególne mechanizmy muszą być dostępne dla następujących

	systemów operacyjnych: Microsoft Windows 10 (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit), Windows 7 (32-bit, 64-bit),Windows Serwer 2019, Windows Server 2016, Windows Server 2008 R2, Windows Server 2012, 2012 R2, Mac OS X v10.15, OS X v10.14, OS X v10.13, Linux OS, Ubuntu 16.04 i późniejsze, Red Hat 7.4 i późniejsze, CentOS 7.4 i późniejsze. 3. Wymaganym jest aby system ochrony stacji końcowej umożliwiał wysyłanie plików do platformy typu Sandbox zlokalizowanego w chmurze producenta (co najmniej w ilości 300 plików dziennie dla każdej stacji klienckiej) lub w ramach postępowania powinna zostać dostarczona komercyjna platforma typu sandbox - zainstalowana lokalnie i współpracująca z oferowanym rozwiązaniem do ochrony stacji roboczych. Wykonawca dostarczy niezbędne licencje upoważniająca zrealizowania wymaganej powyżej funkcji.
Parametry systemu centralnego zarządzania.	1. Dostarczony system centralnego zarządzania aplikacjami klienckimi musi zapewniać wszystkie wymienione poniżej funkcje. Wymaga się aby elementy wchodzące w skład systemu były zrealizowane w postaci komercyjnych platform wirtualnych lub aplikacji instalowanych na systemach operacyjnych: Microsoft Windows Server 2022, Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2. 2. System powinien umożliwiać automatyczną aktualizację oprogramowania zabezpieczającego na urządzeniach końcowych oraz musi zapewniać mechanizmy integracji z sieciowymi systemami bezpieczeństwa, w tym co najmniej: Firewall, Sandbox. 3. Ponadto wymagane jest aby system zapewniał: • integrację z systemami zarządzania tożsamością użytkowników – co najmniej AD, • definiowanie różnych profilów (wersji konfiguracji) ochrony dla różnych grup użytkowników czerpanych z AD lub definiowanych lokalnie, • zautomatyzowany proces zarządzania aplikacja kliencką, • przygotowywanie paczek instalacyjnych przynajmniej dla systemu Windows 32/64 bit i MacOS w których administrator może określić komponenty dla ochrony stacji roboczych takich jak AV, WebFiler, Skaner Podatności. • możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym, • panel, w którym wyświetlane są wyniki analizy podatności na stacjach roboczych, • panel w którym wyświetlane są informacje o podłączonych i zarządzanych stacjach roboczych, • możliwość wymuszenia patchowania wykrytych podatności na stacjach roboczych, • automatyczne wykrywanie stacji klienckich w grupach roboczych,

	• logowanie zdarzeń z aplikacji klienckich, możliwość ich przeglądania z funkcja filtrów oraz możliwością pobierania logów przez administratora, • generowanie alarmów: związanych z zarządzeniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach oraz w sytuacji zaistnienia zdarzeń związanych z aktywnością złośliwego kodu, aktywności aplikacji botnet z wykorzystaniem komunikacji C&C, nieaktualnej bazy danych dla sygnatur antywirusa. • definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcja przypisywania uprawnień do elementów panelu konfiguracyjnego, • zarządzenie certyfikatami na potrzeby połączeń IPSec VPN oraz SSL VPN, • automatyczne wykrywanie aplikacji zainstalowanych na stacjach klienckich z możliwością filtrowania przynajmniej po producencie i nazwie aplikacji, • możliwość przeniesienia użytkownika przez administratora do kwarantanny i personalizację komunikatu, który wyświetli się użytkownikowi, • możliwość wymuszenia przeskanowania stacji klienckiej za pomocą antywirusa i skanera podatności na żądanie jak i cyklicznie, • możliwość skonfigurowania weryfikacji zgodności (compliance) w celu sprawdzenia czy na stacji końcowej jest aktualna baza sygnatur dla AV, czy jest odpowiednia wersja systemu operacyjnego, czy jest uruchomiony odpowiedni proces. 4. Administrator musi mieć możliwość wykonywania backupu i odtwarzania bazy danych, w oparciu o którą działają elementy system. 5. Centralny system zarządzania musi zapewniać możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora lub w ramach postępowania koniecznym jest dostarczenie odpowiednio zabezpieczonego portalu, za pośrednictwem którego administrator będzie mógł dystrybuować paczki instalacyjne.
Licencje oraz serwisy.	Wykonawca wraz z konsolą centralnego zarządzania dostarczy niezbędne licencje upoważniające do: 1. Zainstalowania i centralnego zarządzania [x] (minimum 25 licencji) aplikacjami klienckimi na stacjach roboczych. 2. Dla wskazanej powyżej ilości stacji roboczych licencje powinny obejmować: a) Web Filtering, Skaner podatności, Software inventory, Remote Access, Centralne zarządzanie na okres minimum 18 miesięcy. System musi być objęty serwisem producenta przez okres minimum 18 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

7) Analizer Logów

Wymagania Ogólne	Wykonawca dostarczy centralny system logowania, raportowania i korelacji, umożliwiający centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).
Parametry wydajnościowe:	1. System musi być w stanie przyjmować minimum 5 GB logów na dzień. 2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów. W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:
Logowanie	1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: 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. 4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 5. 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. 6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
Raportowanie	W zakresie raportowania system musi zapewniać: 1. Generowanie raportów co najmniej w formatach: PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Funkcję definiowania własnych raportów.

Korelacja logów	4. Możliwość spolszczenia raportów. 5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. W zakresie korelacji zdarzeń system musi zapewniać: 1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie vpn, utracone połączenie sieciowe. 4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.
Zarządzanie	1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: alną bazę, Radius, LDAP, PKI. 2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
Serwisy i licencje	Wsparcie: System musi być objęty serwisem producenta przez okres minimum 18 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
Wdrożenie	Wdrożenie musi być prowadzone przez jednego certyfikowanego inżyniera, posiadającego minimum 4 aktywne certyfikaty producenta oferowanego w postępowaniu rozwiązania do zbierania i przechowywania logów na poziomie: • Certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci(NS) • Certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej(PCS) • Certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa(SO) • Certyfikowany Specjalista w zakresie Dostępu Zero Trust(ZTA)

PRZEDMIOTOWE ŚRODKI DOWODOWE	1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): 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. 2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

8) System EDR, XDR zintegrowany z systemem antywirusowy – 200 szt.

Administracja zdalna w chmurze	1. W chmurze producenta. 2. Dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Zabezpieczenie za pośrednictwem protokołu SSL. 4. Mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Komunikacja agenta przy wykorzystaniu HTTP Proxy. 6. Zarządzanie urządzeniami mobilnymi – MDM. 7. Wymuszenie dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Dodanie zestawu uprawnień dla użytkowników w oparciu o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji ma możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. 80 szablonów raportów, przygotowanych przez producenta. 10. Tworzenie grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki zawierają: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Uruchamianie zadań automatycznie, z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych	1. Wsparcie systemów operacyjnych Windows (Windows 10/Windows 11). 2. Wsparcie architektury ARM64. 3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Wbudowana technologia do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Opcja umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Integracja z Intel Threat Detection Technology. 11. 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). 12. Skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 13. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Opcja wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 14. Blokowanie zewnętrznych nośników danych na stacji w tym: 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. 15. Blokowanie nośników wymiennych, bądź grup urządzeń umożliwia użytkownikowi tworzenie reguł dla podłączanych urządzeń w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 16. Moduł HIPS ma 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 samoczynnie przełącza się w tryb pracy oparty na regułach, • tryb inteligentny, w którym powiadomienia będą wyłącznie o

	szczególnie podejrzanych zdarzeniach. 17. Wbudowana funkcja generująca pełny raport na temat stacji, na której zostało zainstalowane, z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 18. Funkcja, generująca taki log, posiada 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 19. Automatyczna, inkrementacyjna aktualizacja silnika detekcji. 20. Tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 21. Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 22. Ochrona antyspamowa dla programu pocztowego Microsoft Outlook. 23. Zapora osobista rozwiązania pracuje w jednym z czterech trybów: • tryb automatyczny –blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, • tryb interaktywny – pyta się o każde nowo nawiązywane połączenie, • tryb oparty na regułach – blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, • tryb uczenia się – automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator konfiguruje czas działania trybu. 24. Moduł bezpiecznej przeglądarki. 25. Przeglądarka automatycznie szyfruje wszelkie dane wprowadzane przez Użytkownika. 26. Praca w bezpiecznej przeglądarce jest wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 27. Zintegrowany moduł kontroli dostępu do stron internetowych. 28. Filtrowanie adresów URL w oparciu o co 140 kategorii i podkategorii. 29. Ochrona przed zagrożeniami 0-day. 30. Na stacjach roboczych: wstrzymanie uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
Ochrona serwera	1. Wsparcie systemów Microsoft Windows Server 2012 i nowszych oraz Linux w tym: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux. 2. Ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Skanowanie dysków sieciowych typu NAS. 5. Wbudowane dwa niezależne moduły heurystyczne – jeden

	wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Opcja wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Automatyczna, inkrementacyjna aktualizacja silnika detekcji. 7. Wykluczanie ze skanowania procesów. 8. Określenie typu podejrzanych plików, jakie będą przesyłane do producenta, w tym pliki wykonywalne, archiwa, skrypty, dokumenty. Dodatkowe funkcje dla ochrony serwerów Windows: 9. Skanowanie plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 10. System zapobiegania włamaniom działający na hoście (HIPS). 11. Skanowanie magazynu Hyper-V. 12. Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 13. Blokowanie zewnętrznych nośników danych na stacji w tym: 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. 14. Automatyczne wykrywanie usług zainstalowanych na serwerze i tworzenie dla nich odpowiednich wyjątków. 15. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 16. Dodawanie wyjątków dla systemu IDS, w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 17. Ochrona przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe funkcje dla ochrony serwerów Linux: 18. Uruchamianie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 19. Lokalna konsola administracyjna nie wymaga do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, wspiera rozwiązanie Dell EMC Isilon. 21. Działa w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta zapewnia podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
Szyfrowanie	1. Instalacja aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit. 2. Wsparcie zarządzania natywnym szyfrowaniem w systemach macOS (FileVault). 3. Autentykacja typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Opcja całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 4. Szyfrowanie danych tylko na komputerach z UEFI.
Ochrona urządzeń	1. Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej,

mobilnych opartych o system Android	jak i na karcie SD, bez względu na ich rozszerzenie. 2. 2 poziomy skanowania: inteligentne i dokładne. 3. Automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Konfigurowanie zaufanej karty SIM. 5. Wysłanie na urządzenie komendy z konsoli centralnego zarządzania, umożliwiającej: • usunięcie zawartości urządzenia, • przywrócenie urządzenie do ustawień fabrycznych, • zablokowania urządzenia, • uruchomienie sygnału dźwiękowego, • lokalizację GPS. 6. Podgląd listy zainstalowanych aplikacji. 7. Blokowanie aplikacji w oparciu o: • nazwę aplikacji, • nazwę pakietu, • kategorię sklepu Google Play, • uprawnienia aplikacji, • pochodzenie aplikacji z nieznanego źródła.
Sandbox w chmurze	1. Ochrona przed zagrożeniami 0-day. 2. Wykorzystywanie do działania chmury producenta. 3. Opcja określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 4. Definiowanie po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 5. Definiowanie maksymalnego rozmiaru przesyłanych próbek. 6. Tworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 7. Po zakończonej analizie pliku, przesyłany jest wynik analizy do wszystkich wspieranych produktów. 8. Podgląd listy plików, które zostały przesłane do analizy. 9. Analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 10. Brak wymogu instalacji dodatkowego agenta na stacjach roboczych. 11. Wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator ma podgląd jakie pliki zostały wysłane do analizy oraz przez kogo. 12. Przeanalizowane pliki są odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: • Czysty, • Podejrzany, • Bardzo podejrzany, • Szkodliwy. 13. W przypadku stacji roboczych opcja wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z

	archiwum. 14. W przypadku serwerów pocztowych opcja wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. 15. Wykryte zagrożenia są przeniesione w bezpieczny obszar kwarantanny, z której można przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.
Moduł XDR	1. Dostęp do konsoli centralnego zarządzania odbywa się z poziomu interfejsu WWW. 2. Wysyłanie zdarzeń do konsoli administracyjnej ESET. 3. Interfejs jest zabezpieczony za pośrednictwem protokołu SSL. 4. Wprowadzanie wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 5. Wykluczenia dotyczą procesu lub procesu „rodzica”. 6. Utworzenie wykluczenia automatycznie rozwiązuje alarmy, które pasują do utworzonego wykluczenia. 7. Kryteria wykluczeń są konfigurowane w oparciu o: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 8. Serwer posiada ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator może utworzyć własne reguły i edytować reguły dodane przez producenta. 9. Blokowanie plików po sumach kontrolnych. W ramach blokady można dodać komentarz oraz konfigurację wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 10. Weryfikacja uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu 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. 11. W ramach plików wykonywalnych oraz plików DLL, opcja ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 12. Weryfikacja uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Oznaczanie skryptu jako bezpieczny lub niebezpieczny. 13. W ramach przeglądania wykonanego skryptu, możliwy szczegółowy podgląd wykonanych przez skrypt czynności w formie tekstowej. 14. W ramach przeglądania wykonanego skryptu lub pliku exe, możliwa weryfikacja powiązanych zdarzeń dotyczących: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. 15. Przekierowanie do konsoli zarządzającej ESET, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli ESET, możliwy podgląd informacji dotyczącychj: podzespołów zarządzanego PC (w tym: producent, model, numer seryjny, informacje o systemie, procesor, peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich. 16. Tagowanie obiektów. 17. Połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
Licencja	
Licencja	1. Minimalna ilość wymaganych licencji nie może być mniejsza niż 200. 2. Okres ważności licencji – minimum 18 miesięcy

9) Oprogramowanie DLP – 200 szt.

Minimalne wymagania techniczne	1. System operacyjny: a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi c. MacOS 12 lub nowszy. 2. Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 (64-bit) i nowszych. 3. Serwer administracyjny musi obsługiwać bazy danych: a. MS SQL Server 2016 lub nowsze, b. MS SQL Express, c. AzureSQL S3 lub nowsze. 4. Pomoc i dokumentacja programu dostępne w języku angielskim. 5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim. 6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta. 7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych. 8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym. 9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia. 10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli. 11. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit. 12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania. 13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu. 14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu). 15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory. 16. System musi rejestrować zdarzenia aktywności stacji roboczej, takie jak logowanie, wylogowanie, włączenie, wyłączenie, blokada, odblokowanie i przejście w stan bezczynności. 17. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym. 18. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa. 19. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.

	20. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików. 21. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych. 22. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email. 23. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu. 24. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania. 25. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików. 26. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku. 27. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych, jak i sieciowych. 28. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp. 29. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN. 30. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym. 31. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM. 32. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP. 33. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania. 34. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365. 35. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams. 36. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach 37. Minimalna ilość wymaganych licencji nie może być mniejsza niż 200. 38. Okres ważności licencji – bezterminowe 39. Okres ważności suportu producenta – minimum 18 miesięcy

10) System do zarzadzania czynnościami użytkowników i sprzętu – 200 szt.

Zarządzanie zasobami	
Pozyskiwanie informacji o sprzęcie, zarządzanie	1. Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania

widokami, funkcje ogólne	2. Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP oraz SNMP 3. Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu 4. Operacyjnego wraz z informacją o aktualizacji 5. Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy 6. Odwzorowanie struktury organizacji w oparciu o Active Directory 7. Jednostronna synchronizacja komputerów oraz drukarek z AD oraz AAD (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory) 8. Automatyczne skanowanie całości lub wybranych grup Active Directory (oraz AAD) oraz sieci 9. Mapowanie atrybutów obiektów AD (oraz AAD) do obiektów Statlook 10. Grupowanie wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów, lokalizacji, statusów) 11. Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.) 12. Utworzenie własnych typów elementów wyposażenia 13. Łączenie elementów wyposażenia w zestawy 14. Przypisywanie zasobu do wielu zestawów 15. Makrodefinicje w celu spersonalizowania nazw elementów w drzewku wyposażenia 16. Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach 17. Podpięcie dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików 18. Przypisywanie sprzętu do konkretnych osób 19. Przypisywanie sprzętu do wybranej firmy 20. Automatyczne wyznaczanie 'Głównego użytkownika' komputera 21. Wiązanie wielu rekordów wyposażenia z użytkownikiem 22. Przypisywanie sprzętu do dowolnej lokalizacji 23. Definiowanie własnych, dowolnych atrybutów sprzętu 24. Aktywnym komputerom (bez określonego statusu) przydzielany jest status 'W użyciu' 25. Wydruk etykiet z kodami kreskowymi do inwentaryzacji wyposażenia 26. Dowolna treść kodu kreskowego 27. Określanie loga firmy oraz użycia go na wydrukach 28. Grupowa zmiana domeny/grupy roboczej zasobu
Informacje o sprzęcie	1. Automatyczne wykrywanie typu komputera (Desktop\Notebook\Serwer\Kontroler domeny) na podstawie wyników skanowania sprzętu 2. Wykrywanie komputerów typu All-In-One 3. Automatyczne wykrywanie typów stacji roboczej (Tower\Desktop\SFF\uSFF) 4. Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu

	5. Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM 6. Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany 7. Definiowanie statusów dla sprzętu (Nowy, Do kasacji, W serwisie, itd.) 8. Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc.) 9. Odczyt informacji o module TPM 10. Odczyt D3Dscore z WinSAT 11. Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: Switch, Router, Access Point, Bridge, Modem, NAS, UPS, itd.) 12. Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu 13. Automatyczne wykrywanie i tworzenie monitorów (producent, numer seryjny, rozdzielczość, odczyt firmy, działu, osoby odpowiedzialnej, głównego użytkownika) 14. Automatyczne tworzenie zestawów: Komputer + Monitor 15. Automatyczne utworzenie zestawów: Komputer + drukarka lokalna 16. Automatyczne utworzenie zestawów: host + maszyny wirtualne 17. Automatyczne wykrywanie czy komputer jest maszyną wirtualną 18. Wykrywanie maszyn wirtualnych typu: Parallels Virtual Platform 19. Określanie informacji o wykorzystywanej wirtualizacji 20. Podgląd zestawów, do których należy zasób 21. Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami 22. Przypisywanie stałego atrybutu COA, który będzie uwzględniany na raportach wyposażenia i audytu 23. Definiowanie szczegółowych informacji finansowych 24. Obsługa walut w danych finansowych 25. Definiowanie bazy dostawców sprzętu i oprogramowania 26. Automatyczne odczytywanie ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu) 27. Automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta 28. Agent odczytuje identyfikator SID komputera 29. Określanie adresu interfejsu webowego urządzenia sieciowego 30. Określanie typu gwarancji dla zasobu 31. Określenie wpływu biznesowego wybranego zasobu 32. Tworzenie własnych typów gwarancji 33. Określanie ikony dla typów zasobów 34. Integracja z Dell API 35. Wyszukiwanie i identyfikacja duplikatów zasobów 36. Geolokalizacja komputerów z agentem
Raporty zasobów	1. Raport dodanych załączników 2. Automatyczne tworzenie historii zmian sprzętu 3. Raport zbiorczy historii zmian w sprzęcie 4. Ewidencja zdarzeń serwisowych 5. Dodawanie notatek\komentarzy dla zdefiniowanych obiektów zasobów 6. Informacja na temat pojemności dysków twardych oraz wolnego

	miejsca 7. Wydruk\dodawanie jako załącznik protokołu przekazania\zwrotu\utylizacji sprzętu 8. Wydruk\dodawanie jako załącznik protokołu przekazania dla całego zestawu 9. Kreator szablonów wydruków WYSIWYG 10. Definiowanie dedykowanych profili protokołów 11. Zapisywanie protokołów podczas generowania jako załącznik do zasobu 12. Wydruk\dodawanie jako załącznik Karty informacyjnej do elementu wyposażenia 13. Wydruk lub zapis do pliku raportów ze szczegółami sprzętu 14. Porównywarka wyników skanowania sprzętu 15. Dzienniki zdarzeń systemu Windows 16. Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu 17. Geolokalizacja komputerów z agentem
Zarządzanie zasilaniem	1. Zdalne włączanie i wyłączenie komputerów 2. Obsługa SecureOn przy WakeOnLan 3. Tworzenie harmonogramów wyłączania i włączania komputerów 4. Wybór 5 trybów zamknięcia systemu: Blokada komputera, Uśpienie, Hibernacja, Wyłączenie, Wymuszenie wyłączenia, Restart 5. Możliwość anulowania /wyświetlenia komunikatu jeśli jest zalogowany użytkownik 6. Możliwość przerwania / odłożenia zadania na żądanie użytkownika 7. Wymuszenie wylogowania użytkownika przed wyłączeniem komputera 8. Raport zadań jednorazowych oraz harmonogramów 9. Monitoring obciążenia CPU
Funkcje dodatkowe	1. Zdalne wykonywanie skryptów (batch/powershell) - Obsługa zadań jednorazowych i cyklicznych 2. Podpisywanie skryptów Powershell certyfikatem 3. Wykonywanie skryptów w kontekście sesji użytkownika lub usługi 4. Skrypty wykonywane po uruchomieniu komputera lub zalogowaniu użytkownika 5. Wykonywanie zadań dla wszystkich komputerów 6. Edytor skryptów z funkcją kolorowania składni 7. Wykorzystywanie predefiniowanych skryptów 8. Import informacji o wyposażeniu z pliku CSV 9. Wyszukiwanie sterowników, informacji o komputerze, informacji o gwarancji w bazie producenta (DELL) 10. Mechanizm automatycznego tworzenia rekordów producenta sprzętu (na podstawie wyników skanowania sprzętu) 11. Generowanie kodów paskowych, QR dla każdego elementu wyposażenia 12. Obsługa kodów QR 13. Archiwum zasobów 14. Przeniesienie utylizowanego wyposażenia do archiwum 15. Automatyczne usunięcie informacji sieciowych oraz licencji agenta dla zasobu archiwizowanego

	16. Zarządzanie sprzętem przez aplikacje mobilną 17. Powiadomienia o kończącej się gwarancji\umowie serwisowej dla zasobu 18. Zachowanie ostatniego skanu sprzętu podczas konserwacji bazy danych 19. Powiadomienia o utworzeniu monitora, wykryciu maszyny wirtualnej 20. Grupowa zmiana atrybutów 21. Personalizacja statusów zasobów
Zarządzanie oprogramowaniem	
Licencje	1. Inwentaryzacja licencji 2. Automatyczne tworzenie licencji na podstawie kluczy produktów 3. Odczytu OriginalProductKey (BIOS/UEFI) dla systemu operacyjnego 4. Import licencji z pliku tekstowego 5. Automatyczne generowanie historii zmian w licencji 6. Określanie statusu licencji 7. Tworzenie własnych atrybutów licencji 8. Tworzenie notatek oraz załączników w dowolnym formacie do licencji 9. Tworzenie licencji z poziomu rozliczenia audytu legalności 10. Tworzenie licencji z poziomu raportu kluczy licencji 11. Tworzenie zestawów licencji 12. Relacja licencji z użytkownikiem, firmą, działem, lokalizacją 13. Zmiana typu licencji dla wybranej grupy 14. Kompletna informacja na temat posiadanych licencji (typ, producent, program licencjonowania, czas ważności, informacje finansowe) 15. Przypisywanie licencji do komputera 16. Definiowanie wymaganych atrybutów legalności (faktura, nośnik, COA, etc.) 17. Definiowanie ilości posiadanych licencji w rozbiciu na użytkowników oraz stanowiska 18. Definiowanie licencji przeznaczonych do przyszłego zakupu 19. Definiowanie kluczy seryjnych i przypisywanie do licencji 20. Automatyczne usunięcie wiązania pomiędzy zasobem archiwizowanym a licencją 21. Określenie wpływu biznesowego wybranej licencji
Skanowanie oprogramowania	1. Skanowanie oprogramowania na podstawie harmonogramu oraz definicji skanera 2. Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecania skanów 3. Śledzenie zmian w stanie zainstalowanego oprogramowania 4. Zdalny skan komputerów (bieżący lub okresowy) 5. Zmiana priorytetu skanowania oprogramowania 6. Skan komputerów niepodłączonych do sieci 7. Wysyłanie wyników skanowania offline na serwer FTP (Audyt) 8. Przekazywanie konfiguracji wzorcowej dla skanera offline 9. Identyfikacja zainstalowanych aplikacji na podstawie wzorców oprogramowania 10. Prawidłowe rozpoznanie aplikacji nawet mimo zmiany jej nazwy 11. Określanie masek plików dla publikacji elektronicznych (e-book) 12. Skan plików skompresowanych

	13. Skan oraz identyfikacja zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lzh, lzma, msi, nrg, rar, tar, taz 14. Wbudowane profile skanowania (np. profil wzorcowy) 15. Definicja własnych ustawień skanowania 16. Porównywanie wyników skanowania oprogramowania 17. Wykrywanie plików multimedialnych 18. Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika) 19. Odczytywanie informacji o składnikach aplikacji, których programy instalacyjne nie są zgodne ze standardem MSI 20. Identyfikacja SID użytkownika, dla którego zainstalowano oprogramowanie 21. Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji\pakietów\systemów operacyjnych 22. Nadpisanie bazy wzorców najnowszą, oficjalną bazą producenta 23. Definiowanie katalogów wykluczonych / uwzględnionych w skanowaniu z wykorzystaniem symboli wieloznacznych (* , %)
Audyt oprogramowania	1. Rozliczanie pakietów aplikacji 2. Rozliczanie systemów operacyjnych 3. Rozliczanie licencji typu „Downgrade”, "Upgrade" oraz instalacji innego oprogramowania w ramach licencji 4. Audyt oprogramowania rozliczany automatycznie - informacja o stanie posiadanych licencji i faktycznie zainstalowanych programach z uwzględnieniem wybranych zestawów licencji. 5. Historia audytów (Wyniki audytów są przechowywane w bazie danych - można do nich wracać w dowolnej chwili, porównywać je i generować stosowne raporty) 6. Wsparcie procesu Audytu przez zaimportowanie materiału zdjęciowego i jego obróbkę 7. Gotowe metryki audytowanego komputera - załącznik do protokołu przekazania stanowiska komputerowego (sprzęt + oprogramowanie) 8. Uwzględnianie w rozliczeniu oprogramowania liczby aktywacji zapisanej w szablonie licencji
Funkcje	1. Mechanizm informujący o nowej bazie wzorców oprogramowania 2. Definiowanie własnych wzorców oprogramowania 3. Automatyczne tworzenie wzorców oprogramowania dla systemów operacyjnych 4. Automatyczne dodawanie informacji o wydawcy oprogramowania dla nowych wzorców, tworzonych na podstawie wyników skanowania 5. Wykrywanie kluczy/identyfikatorów programów 6. W przypadku aktywacji systemu Windows z użyciem serwera KMS, klucza MAK (Multiple Activation Keys) lub VLK (Volume License Keys) odczytywane jest 5 ostatnich znaków klucza 7. Odczytywanie informacji o częściowych kluczach pakietów Microsoft Office 8. Drukowanie lub zapisywanie do pliku raportów ze szczegółami oprogramowania 9. Zbiorcze raporty wyników skanowania oprogramowania - Pakiety, pliki, systemy operacyjne, kluczy zainstalowanych aplikacji

	10. Raport z informacjami o pakietach oprogramowania uwzględniający parametry: przybliżona wielkość, adres strony internetowej, lokalizacja pliku instalacyjnego, architektura aplikacji, itd. 11. Raport z informacjami o systemach operacyjnych uwzględniający parametry: Data instalacji, Architektura systemu, Wersja kompilacji, itd. 12. "Wielkie raporty" (Możliwość utworzenia zbiorczych raportów obejmujących np. wszystkie przeskanowane pliki) 13. Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (*.msi) 14. Zdalna dezinstalacja oprogramowania 15. Utworzenie harmonogramu dezinstalacji oprogramowania 16. Generowanie skryptu deinstalacji aplikacji na podstawie otrzymanych wyników skanowania oprogramowania 17. Raport stanu oprogramowania antywirusowego, anty-szpiegowskiego oraz zapory sieciowej 18. Raport zainstalowanych aktualizacji systemu Windows
Kontrola wykorzystania sprzętu i oprogramowania	
Pozyskiwanie informacji o użytkownikach, zarządzanie widokami, funkcje ogólne	1. Dane gromadzone dla konkretnych użytkowników (na bazie kont Windows) - jeden użytkownik może mieć przypisanych wiele kont Windows i pracować na różnych komputerach 2. Odczyt informacji o kontal lokalnych komputera, wraz z odczytem grup do, których konto należy 3. Grupowanie użytkowników z podziałem na jednostki organizacyjne w firmie (np. względem działów) 4. Określanie firmy do której należy użytkownik 5. Określanie przełożonego dla użytkownika 6. Prezentacja 'stanu użytkownika' (obecny, nieobecny, nowy). 7. Prezentacja 'statusu użytkownika' (Zatrudniony, zwolniony, itd.) 8. Zarządzanie stanowiskami użytkowników 9. Przeniesienie rekordu użytkownika do archiwum 10. Funkcjonalności automatycznego generowania zmian rekordu użytkownika – Historia użytkownika 11. Odczytywanie informacji o użytkownikach z Active Directory oraz AAD 12. Pełna synchronizacja rekordów użytkowników (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory oraz AAD) 13. Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień 14. Podgląd zdjęcia przypisanego do użytkownika 15. Przypisywanie do użytkownika załączników (pliki) 16. Przypisywanie notatek do użytkownika 17. Ewidencja zdarzeń przypisanych do użytkowników 18. Automatyczne tworzenie działów na podstawie informacji odczytanych z Active Directory
Raporty	1. Analiza aktywności użytkowników 2. Grupowanie danych według komputerów jeśli użytkownik wykorzystywał więcej niż jedno stanowisko 3. Analiza zdarzeń sesji użytkownika (Logowanie, Wylogowanie,

	Zablokowanie, Odblokowanie, Nawiązanie połączenia RDP, Zakończenie połączenia RDP) 4. Analiza przerw w pracy 5. Analiza jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków) 6. Analiza aktywności mikrofonu oraz kamery 7. Analiza wykorzystania poszczególnych aplikacji w czasie 8. Analiza czasu działania aplikacji, na pierwszym planie oraz sumarycznie 9. Uwzględnienie lub wyłączenie z raportu aplikacji bez aktywności użytkownika 10. Kategoryzacja danych czasu pracy (czas pozytywny, neutralny oraz negatywny). 11. Statystyki najczęściej wykorzystywanych aplikacji 12. Statystyki wykorzystania komputerów przez poszczególnych użytkowników 13. Statystyki aktywności użytkownika i grup użytkowników 14. Generowanie raportów z monitoringu użytkowników dla wybranego zakresu godzin 15. Kontrola wydruków - historia zadań drukowania zainicjowanych przez poszczególnych użytkowników 16. Kontrola wydruków - Monitoring wydruków obejmuje szczegółowe parametry (np. format papieru, orientacje, skalowanie, itd.) 17. Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz-b/kolor, dpi) 18. Monitoring wydruków na drukarkach sieciowych 19. Monitoring użytkowników stacji terminalowych 20. Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.) 21. Informacje o awariach, poczynaniach użytkowników: zakończonej aktualizacji, akcji podpięcia przenośnych dysków, włożenia płyt do napędów CD/DVD, śledzenie uruchomienia aplikacji przez użytkownika, monitoring informujący o małej ilości miejsca 22. Raport zbiorczy historii zmian w rekordach użytkowników
Funkcje	1. Blokada niepożądanych aplikacji. Programy mogą być blokowane dla całej firmy lub tylko dla wybranych użytkowników. 2. Autoryzacja nośników zewnętrznych na podstawie wykrytych urządzeń 3. Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych 4. Automatycznie budowana baza informacji o napędach zewnętrznych 5. Blokada dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.) 6. Odczyt i blokada urządzeń PTP/MTP 7. Określanie praw dostępu w zależności od typu urządzenia, np. Pendrive, CD/ROM 8. Komunikacja z użytkownikami (Skype, mail) bezpośrednio z zakładki Użytkownicy 9. Informacje o ostatnio zalogowanych osobach na stacjach klienckich 10. Automatyczne tworzenie licencji – Dodawanie do licencji użytkowników, którzy są głównymi użytkownikami komputera, na którym wykryto licencje 11. Komentowanie przerw pracy

	12. Kategoryzacja przerwy w pracy na podstawie komentarza
Kontrola wykorzystania Internetu	
Funkcje	1. Blokada stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokada WWW po zawartości (ContentType) 2. Blokada stron internetowych dla protokołu http \ https w najpopularniejszych przeglądarkach WWW 3. Kategoryzacja stron internetowych 4. Import stron WWW z pliku lub ze schowka 5. Slowniki kategorii stron WWW 6. Blokada dostępu do witryn zgodnie z harmonogramem 7. Blokada trybu incognito w przeglądarce Google Chrome
Raporty	1. Raporty dotyczące aktywności użytkowników w Internecie 2. Analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki) 3. Monitoring stron internetowych dla protokołu http \ https (Edge, Chrome, Opera, Vivaldi, Firefox) 4. Analiza liczby wejść na poszczególne strony lub domeny 5. Kategoryzacja odwiedzanych domen i stron 6. Raport informujący o plikach pobranych przez przeglądarki WWW 7. Raport informujący o danych wysłanych przez przeglądarki (bez Firefox) 8. Monitoring plików pobieranych przez przeglądarki internetowe
Helpdesk	
Obsługa	1. Rejestracja i obsługa zgłoszeń 2. Obsługa zgłoszeń w modelu Kanban 3. Określanie relacji pomiędzy zgłoszeniami (np.. Kopia, Incydent nadrzędny) 4. Edycja zgłoszeń powiązanych w oknie zgłsozenia bieżącego 5. Kategoria zgłoszeń może posiadać swojego opiekuna, który może zarządzać każdym zgłoszeniem danej kategorii 6. Komentarze zgłoszenia obsługujące HTML oraz osadzanie obrazów 7. Opis zgłoszenia w formacie HTML 8. Nawiązywanie połączeń zdalnych bezpośrednio z edytora incydent 9. Tworzenie notatek dla zgłoszeń 10. Zapisywanie wersji roboczej komentarza 11. Archiwizacja zgłoszeń 12. Monitoring czasu pracy nad incydentem (time tracking) 13. Raport ewidencji czasu pracy nad zgłoszeniem 14. Informacja o czasie reakcji do podjęcia zgłoszenia 15. Dodanie prywatnego komentarza 16. Znaki @ oraz # pozwalają na wspominanie użytkownika oraz wpisu bazy wiedzy w komentarzu zgłoszenia 17. Dodanie załączników do incydentów, również do komentarza 18. Określanie dodatkowych subskrybentów dla notyfikacji e-mail dotyczącej zmian w incydencie 19. Określanie uprawnień do incydentów (Publiczne, Prywatne, dla określonych działów) 20. Zarządzanie filtrami zdefiniowanymi dla listy zgłoszeń

	21. Obsługa nazwy DNS oraz adresów IP (IPv4, IPv6) dla zgłoszeń 22. Wydruk historii zgłoszenia 23. Widok kalendarza (Planowanie rozwiązania incydentów) 24. Korelacja incydentu z elementem zasobów 25. Raport zbiorczy historii zmian 26. Tworzenie i planowanie zastępstw, osoba zastępująca otrzymuje na czas zastępstwa dostęp do obsługi zgłoszeń osoby zastępowanej 27. Wyszukiwanie komentarzy przy użyciu funkcji globalnego wyszukiwania 28. Czas reakcji oraz realizacji wyznaczany automatycznie na podstawie umów SLA 29. Automatyczne podpowiedzi rozwiązań dostępnych w bazie wiedzy na podstawie wpisywanego tematu 30. Określenie wpływu biznesowego wybranego zgłoszenia 31. Podgląd wiadomości źródłowej przy tworzeniu zgłoszenia lub komentarza na podstawie zgłoszeń email 32. Duplikacja i replikacja zgłoszeń 33. Powiadomienia o liczbie nieprzeczytanych zgłoszeń 34. Automatyzacja obsługi zgłoszeń z wykorzystaniem utworzonych reguł
Konfiguracja	1. Architektura drzewa dla kategorii zgłoszeń 2. Tworzenie szablonów odpowiedzi 3. Cykliczne raportowanie Listy incydentów 4. Tworzenie własnych dodatkowych atrybutów dla zgłoszeń 5. Personalizowane szablony wiadomości email z możliwością ustawienia stałego załącznika 6. Notyfikacje e-mail o utworzeniu\zmianie\usunięciu incydentu 7. Notyfikacje e-mail o zbliżających się terminach realizacji incydentu (Deadline) 8. Automatyczny import wiadomości e-mail, jako zgłoszeń helpdesk (POP3 oraz IMAP) 9. Import zgłoszeń helpdesk ze skrzynek współdzielonych (shared mailbox) 10. Obsługa wielu kont pocztowych (Import + notyfikację email) 11. Tworzenie własnych trybów oraz priorytetów incydentów 12. Personalizacja widoku raportu listy incydentów 13. Profile zgłaszających w helpdesk 14. Personalizacja kolorów statusów zgłoszeń 15. Automatyczne przypisywanie zgłoszeń do użytkowników 16. Weryfikacja wiadomości źródłowych pobieranych z serwera pocztowego 17. Konfiguracja maksymalnej wielkości załącznika
Moduł połączeń zdalnych	1. Operacje na plikach i katalogach 2. Zarządzanie procesami i rejestrem 3. Monitoring pracy wykonywanej na komputerze 4. Zdalny podgląd pulpitów wielu stacji (Funkcja Company Online) 5. Wywoływanie Windows Remote Desktop na danej stacji z poziomu aplikacji 6. Wysyłanie wiadomości do użytkowników 7. Uruchamianie na stacjach programów z wiersza poleceń Command

	Line 8. Zdalne uruchamianie komputera za pomocą funkcji Wake-On-Lan 9. Wake-On-Lan pozwala na definicję portu oraz adresu komputera docelowego 10. Przejęcie kontroli nad stacją roboczą 11. Blokada klawiatury i myszki na stacji klienckiej w trakcie przejęcia kontroli pulpitu zdalnego 12. Przesyłanie kombinacji klawiszy Ctrl + Alt + Delete w zdalnym pulpicie 13. Przejęcie kontroli nad komputerem bez zalogowanego użytkownika 14. Wysyłanie pytania o zgodę na zdalny dostęp lub wysyłania komunikatu z informacją o rozpoczęciu podglądu pulpitu 15. Podgląd pulpitu zdalnego w osobnym oknie z opcją fullscreen 16. Obsługa wielu monitorów dla podglądu pulpitu 17. Wybór monitora, z którego ma być przekazywany obraz podglądu pulpitu 18. Nawiązywanie połączenia pulpitu zdalnego z wieloma komputerami jednocześnie 19. Połączenie pulpitem zdalnym w konfiguracji NAT-NAT 20. Zarządzanie usługami systemu Windows 21. Raport Sesje zdalnego pulpitu 22. Wybór adresu IP, na którym ma być zestawione połączenie DirectPC 23. Wybór portu, na którym klient nasłuchuje połączenia zdalnego 24. Wykorzystanie protokołu autorskiego lub MS RDP do połączeń zdalnych
Baza wiedzy	1. Wbudowana baza wiedzy 2. Artykuły bazy wiedzy mogą być przypisane do kategorii zgłoszeń helpdesk 3. Kopiowanie artykułów 4. Edytor HTML 5. Osadzanie załączników w treści artykułów 6. Osadzanie multimediów w treści artykułów 7. Baza wiedzy pozwala na tworzenia artykułów prywatnych oraz publicznych 8. Szybkie kopiowanie wpisów bazy wiedzy 9. Artykuły bazy wiedzy mogą zostać powiązane ze zgłoszeniami z systemu helpdesk 10. Artykuły bazy wiedzy mogą zostać przypięte, dzięki czemu zawsze będą widoczne na liście artykułów 11. Informacja o liczbie odsłon artykułu bazy wiedzy 12. Bezpośrednie linkowanie artykułów bazy wiedzy
SLA	1. Definiowanie planów umów SLA 2. Definiowanie czasu obowiązywania umów SLA 3. Definiowanie czasu pracy działów wsparcia technicznego 4. Definiowanie dni wolnych na podstawie kalendarza świąt i dni wolnych 5. Definiowanie czasów reakcji oraz realizacji zgłoszenia 6. Notyfikacje mailowe o zbliżających się terminach reakcji oraz realizacji 7. Automatyczne przypisanie umowy SLA do zgłoszenia na podstawie informacji o rozwiązującym, temacie wiadomości, priorytecie, kategorii, opisie 8. Raportowanie o statusie i postępie w realizacji zgłoszeń z przypisaną

	umową SLA
Centralne repozytorium załączników	
Funkcje	1. Załączniki przechowywane w centralnym repozytorium 2. Utworzenie relacji załącznika z innymi elementami systemu 1 - N (jeden do wielu) 3. Dodawanie i modyfikacja załączników z poziomu innych zasobów 4. Załączniki typu: link, udział oraz plik 5. Pełna informacja o załączniku: twórca, data utworzenia, rozmiar, nazwa pliku, miniatura 6. Historia zmian załącznika
Zarządzanie użytkownikami	
Funkcje	1. Raportowanie aktywności pracy 2. Przeglądanie ostatnio zgłoszonych incydentów 3. Powiązanie użytkownika z licencją 4. Dostęp webowy do statystyk monitoringu, zgłoszeń helpdesk oraz powiązanych z użytkownikiem zasobów 5. Cykliczne, automatyczne generowanie raportów 6. Generowanie raportu obecności / nieobecności użytkownika wraz z korelacją jego aktywności na komputerze 7. Zgłoszenia dotyczące wniosków nieobecności użytkowników 8. Automatyczne typowanie użytkowników zastępujących dla zgłaszanych nieobecności 9. Zarządzanie wnioskami nieobecności użytkowników przez przełożonych, informowanie przełożonych N poziomów wyżej o urlopie użytkownika 10. Automatyczne utworzenie relacji przełożony - podwładny na podstawie skanów Active Directory 11. Możliwość drukowania karty informacyjnej użytkownika, zawierającej informacje kontaktowe, informacje o powiązanych zasobach, licencjach oraz dostępy nadane w module RODO 12. Generator struktury organizacji na podstawie powiązań użytkowników i ich przełożonych 13. Planowanie dni wolnych w widoku kalendarza 14. Planowanie zastępstw podczas nieobecności
Raportowanie cykliczne	
Użytkownicy	1. Raport historia sesji 2. Raport Nośniki danych 3. Raport Operacje na plikach 4. Raport wydruków 5. Raport użycia aplikacji 6. Raport nagłówów okien 7. Raport odwiedzonych stron WWW 8. Najczęściej odwiedzane strony internetowe 9. Raport Wysyłane pliki 10. Raport czasu pracy przy komputerze 11. Raport Bizlook
Zasoby	1. Raport historii zasobów 2. Raport informujący o nowych zasobach 3. Raport informujący o nadchodzących terminach w zasobach

	4. Raport Zasoby zarchiwizowane 5. Raport Systemy Operacyjne
Podstawowe	Raport Informacje o autoryzowanych agentach
Oprogramowanie	1. Raport zainstalowanego oprogramowania 2. Raport Szczegóły plików
Helpdesk	1. Raport incydentów (Helpdesk) 2. Raport czasu pracy nad zgłoszeniem 3. Raport Czasy SLA
Automatyzacja	
Lista dostępnych reguł	
Ogólne	1. Zakończenie asysty serwisowej AS lub AS Plus 2. Wygaśnięcie certyfikatu SSL 3. Kończące się licencje na agenta 4. Zapełniona baza danych 5. Zbyt duży rozmiar folderu cache
Zasoby	1. Brak połączenia od agenta 2. Brak wolnej przestrzeni na dysku 3. Ostrzeżenie od Windows Security Center 4. Zakończenie skanowania sprzętu 5. Dodanie zasobu 6. Zmiana zasobu 7. Usunięcie zasobu 8. Zakończenie okresu gwarancyjnego 9. Zakończenie umowy serwisowej 10. Powielenie zasobów
Oprogramowanie	1. Zmiana oprogramowania 2. Zakończenie skanowania oprogramowania 3. Zamknięcie audytu
Licencje	1. Dodanie licencji 2. Zmiana licencji 3. Usunięcie licencji 4. Wygaśnięcie licencji 5. Planowana wymiana licencji
Użytkownicy	1. Dodanie użytkownika 2. Zmiana użytkownika 3. Usunięcie użytkownika 4. Logowanie użytkownika 5. Wylogowanie użytkownika
Helpdesk	1. Dodanie zgłoszenia 2. Usunięcie zgłoszenia 3. Zmiana zgłoszenia 4. Brak aktywności w zgłoszeniu
Lista dostępnych Akcji	1. Wykonywanie skryptu na podstawie zdefiniowanej reguły 2. Wysłanie powiadomienia w konsoli Master / Statlook Web na podstawie zdefiniowanej reguły 3. Wysyłanie powiadomienia mailowego na podstawie zdefiniowanej reguły (inicjator zdarzenia, Administratorzy, konkretny użytkownik, rozwiązujący, zgłaszający, subskrybenci)

	4. Modyfikacja zasoby / użytkownika / zgłoszenia - w zależności od reguły 5. Dodanie komentarza (dla reguł Helpdesk) 6. Wysyłka wiadomości SMS
RODO	
Funkcje	1. Inwentaryzacja zbiorów danych, dostępów oraz powierzeń do zbiorów danych, dokumentów bezpieczeństwa, historii naruszeń bezpieczeństwa, szkoleń oraz wniosków o zapomnienie 2. Wydruk raportów tabelarycznych: czynności przetwarzania, dostępów, powierzeń, listy dokumentów, statystyki zgłoszeń RODO, listę szkoleń, historii naruszeń bezpieczeństwa, wniosków o zapomnienie 3. Wydruk wniosków o nadanie uprawnień, modyfikacji oraz anulowania upoważnienia 4. Wstępne wypełnienie wniosków o zmianę dostępu 5. Utworzenie zgłoszeń za pomocą przycisków szybkiej akcji 6. Delegowanie zadań w helpdesk dla osób odpowiedzialnych za zbiory danych 7. Archiwizacja zbiorów 8. Definiowanie czynności przetwarzania 9. Przypisywanie zbioru danych do czynności przetwarzania 10. Przydzielanie dostępów do czynności przetwarzania 11. Zapisywanie historii zmian wniosków o dostęp do zbiorów 12. Dodawanie historycznych dostępów oraz wniosków o dostęp 13. Filtrowanie użytkowników w raporcie Dostępy
Raporty	1. Raport zbiorczy Czynności przetwarzania 2. Raport zbiorczy Zbiory danych 3. Raport zbiorczy zinwentaryzowanych dostępów 4. Raport zbiorczy zinwentaryzowanych powierzeń 5. Raport zbiorczy zinwentaryzowanych dokumentów 6. Raport zbiorczy historii naruszeń bezpieczeństwa 7. Raport zbiorczy wniosków o dostęp 8. Raport zbiorczy Dostępy
Sygnalista	
Funkcje	1. Tworzenie zgłoszeń w postaci anonimowej lub nieanonimowej 2. Usuwanie metadanych z załączników zgłoszeń 3. Usuwanie danych osobowych ze zgłoszeń 4. Podział interfejsu na publiczny oraz dla wewnętrzny 5. Dashboard podsumowujący wykorzystanie portalu sygnalisty 6. Przypisywanie rozwiązujących zgłoszenia sygnalistów w zależności od typu zgłoszenia lub jego źródła 7. Definiowanie własnych atrybutów, kategorii, trybów zgłoszeń oraz poziomów ryzyka 8. Definiowanie stron publicznych (dostępnych dla sygnalistów) 9. Obsługa wielu języków stron publicznych 10. Natywne wsparcie języka ukraińskiego 11. Definiowany limit załączników 12. Wyróżnienie zgłoszeń o przekroczonym czasie reakcji
Raporty	1. Raport zgłoszeń 2. Historia zmian 3. Statystyka zgłoszeń

	4. Pozostały czas na przyjęcie zgłoszenia 5. Pozostały czas do zakończenia 6. Widgety: Kategorie zgłoszeń, Poziomy ryzyka, Tryby zgłoszeń, Statusy zgłoszeń, Ostatnio dodane
Portal Web	
Funkcje	1. Wallboard - ekran zbiorczy prezentujący wybrane informacje z całego systemu 2. Dashboard każdego modułu z najważniejszymi informacjami w postaci widgetów 3. Widok “Mój dzień” zawierający oś czasu z aktywnością użytkownika 4. Rozbudowane filtry dla raportów tabelarycznych 5. Zarządzanie użytkownikami, agentami, zasobami, licencjami, działami, audytami 6. Konfiguracja portalu helpdesk, kont administracyjnych oraz organizacji 7. Raporty dla każdego modułu w formie tabelarycznej 8. Obsługa helpdesk oraz bazy wiedzy 9. Obsługa modułu RODO 10. Obsługa modułu automatyzacja 11. Obsługa modułu Sygnalita 12. Automatyczne logowanie przy pomocy aplikacji 13. Logowanie za pomocą poświadczeń domenowych (SSO) 14. Logowanie za pomocą konta AzureAD lub AAD 15. Wydruk raportów tabelarycznych 16. Kontrola statystyk użytkowników 17. Menu szybkiego dodawania nowych elementów (użytkownik, nieobecność, zasób, licencja, zgłoszenie, artykuł bazy wiedzy, zbiór danych, czynność przetwarzania) 18. Przełączanie wersji językowej bez ponownego logowania do systemu
Funkcjonalności ogólne	1. Określanie praw dostępu do grup zasobów lub użytkowników 2. Aplikacja desktopowa służąca do zarządzania systemem może być zainstalowana na dowolnej liczbie komputerów ("Licencja pływająca") 3. Dodatkowa aplikacja webowa umożliwiająca dostęp do systemu i zarządzanie systemem 4. Wersja angielska (en-US) interfejsu użytkownika 5. Praca w oparciu o silniki baz danych: MS SQL lub PostgreSQL 6. Swobodna migracja danych pomiędzy MS SQL i PostgreSQL 7. Zdalna instalacja i dezinstalacja agentów na stacjach roboczych 8. Odczytywanie struktury organizacji z Active Directory 9. Skaner sieci wykorzystywany do wykrywania nowych urządzeń 10. Mechanizm automatycznego tworzenia komputera na podstawie danych przesłanych przez agenta 11. Mechanizm automatycznego tworzenia użytkowników na podstawie danych przesłanych przez agenta 12. Automatycznie dodane komputery\użytkowników są powiązane z odpowiednią grupą zgodną z OU w Active Directory 13. Definiowanie nieograniczonej liczby użytkowników systemu 14. Określanie ról dla kont systemu: Administratorzy, Menadżerowie, Zarządcy,Pracownicy 15. Indywidualny login i hasło dla poszczególnych użytkowników

	16. Automatyczne logowanie do systemu 17. Zarządzanie uprawnieniami użytkowników - określanie dostępu do poszczególnych obiektów systemu (konkretny użytkownik, konkretny zasób lub ich grupy) , możliwość ograniczenia operacji (wyświetlanie, tworzenie, edycja, usuwanie) 18. Dostęp do programu chroniony przy pomocy uwierzytelniania wieloskładnikowego 19. Określanie ról użytkowników - zarządzanie grupami 20. Zabezpieczenie Agentów przed nieautoryzowanym wyłączeniem lub usunięciem 21. Eksport danych do plików zewnętrznych (Excel, html, CSV, PDF, TXT, MHT, RTF, BMP) 22. Zgodny z pracą w sieciach WLAN 23. Podgląd aktualnych zadań serwera 24. Centrum informacji - przekrojowy raport na temat zdarzeń oraz statusu monitorowanych komputerów i użytkowników 25. Wielopoziomowe drzewo lokalizacji oraz relacje lokalizacji z firmami 26. Wyszukiwanie danych w tabelach raportów 27. Dowolne definiowania grup sprzętu i użytkowników 28. Tworzenie dowolnych raportów ad-hoc - sortowanie kolumn grupowanie, ukrywanie/odkrywanie kolumn, zaawansowane filtrowanie danych w oparciu o funkcje logiczne 29. Definiowanie i zapamiętywanie własnych widoków 30. Eksport danych bezpośrednio do MS Excel 31. Budowa zestawień metodą drag'n'drop 32. Budowa modułowa z możliwością przypisywania określonych wtyczek programu (funkcji) do poszczególnych Agentów 33. Obsługa protokołu SSL zapewniającego bezpieczną komunikację Master-Serwer oraz Agent-Server. 34. Połączenia pomiędzy komponentami realizowane za pomocą HTTP/HTTPS lub net.TCP 35. Mechanizm kompresji pakietów danych przesyłanych przez Agenta 36. Automatyczne wykrywanie lokalizacji serwera aplikacji (WS-Discovery) 37. Przekazanie agentowi nowych parametrów połączenia z usługą serwera (serwer zapasowy) 38. Definiowanie konfiguracji serwera proxy dla połączenia Agent-Server 39. Mechanizm zdalnego pobierania bieżących aktualizacji do programu 40. Help kontekstowy wraz z podręcznikiem użytkownika w polskiej wersji językowej 41. Dostęp do bazy wiedzy systemu 42. Definiowanie ustawień pracy Agentów (optymalizacja dla dużej liczby komputerów) 43. Dedykowane narzędzie, dostarczane z systemem, do wykonywania kopii bazy danych, niezależnie od wersji silnika bazy danych (MSSQL, PostgreSQL). Uruchomienie narzędzia backupu bazy w trybie wsadowym 44. Manualna i automatyczna konserwacja bazy danych - usuwanie wyników skanowania oprogramowania 45. Personalizacja pakietu instalacyjnego agenta 46. Określanie polityki haseł dla systemu

	47. Zmiana języka systemu podczas logowania 48. Określenie numeru BDO przy definiowaniu rekordu firmy 49. Opcja resetu hasła podczas logowania 50. Globalne wyszukiwanie obiektów w systemie 51. Utworzenie atrybutów jako lista/słownik 52. Podgląd aktualnie zalogowanych użytkowników. Umożliwienie wylogowania wybranych użytkowników 53. Definicja kalendarzy dni wolnych, uwzględnianych w module Helpdesk oraz Monitoring 54. Wyszukiwarka ustawień w opcjach systemowych 55. Instalacja konsoli zarządzającej w kontekście użytkownika (nie wymaga uprawnień administracyjnych) 56. Historia obiektu zawiera informacje o koncie serwisowym, które wprowadziło zmianę w obiekcie 57. Skanowanie lasu domen 58. Budowa personalizowanego pakietu instalacyjnego 59. Automatyczne zamknięcie Statlook Master po zakończeniu sesji 60. Logowanie do portalu Web za pomocą mechanizmu Single Sign On 61. Logowanie operacji kont serwisowych 62. Statlook Security Key - dodatkowa metoda uwierzytelniania klientów przed połączeniem do serwera 63. Logowanie nieudanych prób uwierzytelnienia 64. Eksport danych diagnostycznych oraz dzienników operacji 65. Integracja z SMS API
Dodatkowe informacje	1. Praca w oparciu o MS SQL Server oraz MS SQL Express (2008/2012/2014/2016/2019/2022 32/64 bit) 2. Praca w oparciu o PostgreSQL 10 lub nowszy 3. Szyfrowane połączenie pomiędzy serwerem Statlook a bazą danych 4. Obsługa systemów operacyjnych - Agent: Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, Windows 10, Windows 11 5. Obsługa systemów operacyjnych - Master : Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, Windows 10, Windows 11 6. Obsługa systemów operacyjnych - Serwer: Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8, Windows 10, Windows 11 7. Wszystkie wykonywalne komponenty systemu są podpisane certyfikatem DigiCert Code Signing Certificates for Microsoft Authenticode (Digicert) 8. Sterowniki systemowe są podpisane certyfikatem Extended Validation (EV) Code Signing Certificate (GlobalSign) i mogą pracować w 64-bitowych systemach operacyjnych Microsoft Windows™.
Licencja	
Licencja	1. Minimalna ilość wymaganych licencji nie może być mniejsza niż 200. 2. Okres ważności licencji – bezterminowe 3. Okres ważności suportu producenta – minimum 18 miesięcy

11) i 12) Rozwiązanie do backupu maili sprzęt.

Wymagania ogólne	System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów: 1. Tryb Gateway. 2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).
Parametry fizyczne systemu antyspamowego	1. System musi być wyposażony w interfejsy: • 4 porty Gigabit Ethernet RJ-45. 2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB . 3. System musi posiadać wbudowany port konsoli szeregowej. 4. Zasilanie z sieci 230V/50Hz.
Funkcja serwera poczty	W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 150 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.
Funkcje serwera poczty	W tym zakresie dostarczony system musi zapewniać: 1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP. 2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1 oraz TLS 1.2). 3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników. 4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3). 5. Polski interfejs użytkownika przy dostępie przez WebMail. 6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP. 7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.
Ogólne funkcje systemu ochrony poczty	Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje: 1. Wsparcie dla co najmniej 20 domen pocztowych. 2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 14 tys wiadomości/godzinę. 3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy

	mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all). 4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP. 5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości). 6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie. 7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej. 8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów. 9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP. 10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika. 11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. 12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail. 13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki. 14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. 15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu. 16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. 17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
Kontrola antywirusowa i ochrona przed malware	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Skanowanie antywirusowe wiadomości SMTP. 2. Kwarantannę dla zainfekowanych plików. 3. Skanowanie załączników skompresowanych. 4. Definiowanie komunikatów powiadomień w języku polskim. 5. Blokowanie załączników w oparciu o typ pliku. 6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej. 7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu. 8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. 9. Ochronę typu wirus outbrake.

	10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.
Kontrola antyspamowa	System musi zapewniać poniższe funkcje i metody filtrowania spamu: 1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta. 2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania. 3. Szczegółowa kontrola nagłówka wiadomości. 4. Analiza Heurystyczna. 5. Współpraca z zewnętrznymi serwerami RBL, SURBL. 6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen. 7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników. 8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF. 9. Kontrola w oparciu o Greylisting oraz SPF. 10. Filtrowanie treści wiadomości i załączników. 11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. 12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej. 13. Ochrona typu outbrake. 14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking). 15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata. 16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level). 17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
Ochrona przed atakami na usługę poczty	System musi zapewniać poniższe funkcje i metody filtrowania: 1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing). 2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu. 3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. 4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing). Weryfikacja poprawności adresu e-mail nadawcy.
Funkcje logowania i raportowania	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Logowanie do zewnętrznego serwera SYSLOG. 2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.

	3. Logowanie informacji na temat spamu oraz niedozwolonych załączników. 4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych. 5. Możliwość analizy przebiegu sesji SMTP. 6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. 7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu. 8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
Funkcje pracy w trybie wysokiej dostępności (HA)	System ochrony poczty musi zapewniać poniższe funkcje: 1. Konfigurację HA w każdym z trybów: gateway, transparent. 2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP. 3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu. 4. Monitorowanie stanu pracy klastra.
Aktualizacje sygnatur, dostęp do bazy spamu	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. 2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
Zarządzanie	System ochrony poczty musi zapewniać poniższe funkcje: 1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. 2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy. 3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.
Certyfikaty	Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji: 1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: 1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres minimum 18 miesięcy. Gwarancja oraz wsparcie 2. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 18 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.
Wdrożenie	Wdrożenie musi być prowadzone przez jednego certyfikowanego

	inżyniera, posiadającego minimum 4 aktywne certyfikaty producenta oferowanego w postępowaniu rozwiązania pocztowego na poziomie: • Certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci(NS) • Certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej(PCS) • Certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa(SO) • Certyfikowany Specjalista w zakresie Dostępu Zero Trust(ZTA)
Rozszerzone wsparcie serwisowe	1. System musi być 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 minimum 18 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty: • Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego.
Opisy do wymagań ogólnych	1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): 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. 2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

13) Opracowanie i wdrożenie dokumentacji SZBI oraz KRI, procedur zgodnej z normą 27001 w tym aktualizacja polityk bezpieczeństwa, utworzenie procedury obsługi incydentów, ciągłości działania.

Zakres usługi opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłością Działania wraz z doradztwem w obszarze wdrożenia	
Aktualizacja lub przegląd lub opracowanie lub wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (w skład czego mogą wchodzić różne polityki i procedury)	
Polityka Bezpieczeństwa Informacji:	1. analiza wyników przeprowadzonego audytu wstępnego przez ekspertów; 2. wizyta/wideokonferencja z przedstawicielem jednostki w celu przygotowania dedykowanej Polityki Bezpieczeństwa Informacji; 3. doradztwo we wdrożeniu i bieżące wsparcie ekspertów; 4. przeprowadzenie szkolenia w formie e-learningowej dla całego personelu jednostki w obszarze przyjętej Polityki.
Polityka Zarządzania Systemem Teleinformatycznym:	1. analiza wyników przeprowadzonego audytu wstępnego przez eksperta; 2. wizyta/wideokonferencja z przedstawicielem jednostki w celu przygotowania dedykowanej Polityki Zarządzania Systemem Informatycznym; 3. doradztwo we wdrożeniu i bieżące wsparcie ekspertów; 4. przeprowadzenie szkolenia w formie e-learningowej dla całego personelu jednostki obejmujące wszystkie procesy z obszaru Krajowych Ram Interoperacyjności.
Polityka Zarządzania Ciągłością Działania wraz z Planami Ciągłości Działania w obszarze IT:	1. analiza wyników przeprowadzonego audytu wstępnego przez eksperta; 2. wizyta/wideokonferencja z przedstawicielem jednostki w celu przygotowania dedykowanej Polityki Zarządzania Ciągłością Działania; 3. przygotowanie i przekazanie Polityki Zarządzania Ciągłością Działania wraz z Planami Ciągłości Działania w obszarze IT; 4. doradztwo we wdrożeniu i bieżące wsparcie ekspertów; 5. przeprowadzenie szkolenia w formie e-learningowej dla całego personelu jednostki obejmujące obszar utrzymania ciągłości działania.
Polityka Zarządzania Incydentami Cyberbezpieczeństwa	1. analiza wyników przeprowadzonego audytu wstępnego przez eksperta; 2. wizyta/wideokonferencja z przedstawicielem jednostki w celu przygotowania dedykowanej Polityki Zarządzania Incydentami Cyberbezpieczeństwa; 3. przygotowanie i przekazanie Polityki Zarządzania Incydentami Cyberbezpieczeństwa; 4. przygotowanie i przekazanie Planu Reagowania na Incydenty; 5. przygotowanie i przekazanie Planu Zarządzania Podatnościami; 6. doradztwo we wdrożeniu i bieżące wsparcie ekspertów;

	7. przeprowadzenie szkolenia w formie e-learningowej dla całego personelu jednostki obejmujące wdrożoną Politykę Zarządzania Incydentami Cyberbezpieczeństwa oraz wymogów prawnych wynikających Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r.poz. 913, 1703).
Polityka Ochrony Danych:	1. analiza wyników przeprowadzonego audytu wstępnego przez eksperta; 2. wizyta/wideokonferencja z przedstawicielem jednostki w celu przygotowania dedykowanej Polityki Ochrony Danych; 3. przygotowanie i przekazanie Polityki Ochrony Danych; 4. doradztwo we wdrożeniu i bieżące wsparcie ekspertów; 5. przeprowadzenie szkolenia w formie e-learningowej dla całego personelu jednostki obejmujące wdrożoną Politykę Ochrony Danych oraz omówienie przyjętych procedur zgodnie z przepisami z zakresu ochrony danych w oparciu o przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
Analiza Ryzyka Bezpieczeństwa Informacji	1. analiza wyników przeprowadzonego audytu wstępnego przez ekspertów; 2. wizyta/wideokonferencja z przedstawicielem jednostki w celu przeprowadzenia analizy ryzyka; 3. przygotowanie i przekazanie Raportu z przeprowadzonej analizy ryzyka i omówienie obszarów o podniesionym ryzyku wraz z rekomendacjami ekspertów.
W ramach prowadzonych działań muszą zostać dostosowane / wdrożone następujące procedury / dokumenty:	procedury korzystania z urządzeń mobilnych, procedury pracy zdalnej, postępowanie z nośnikami, procedury kontroli dostępu, zabezpieczenie pomieszczeń i obiektów, procedury czystego biurka, procedury czystego ekranu, procedury kopii zapasowych, procedury ochrony logów, bezpieczeństwo komunikacji, zarządzanie bezpieczeństwem sieci, przesyłanie informacji, plany ciągłości działania, procedury zarządzania incydentami, prywatność i ochrona danych osobowych, szacowanie ryzyka w obszarze bezpieczeństwa informacji, szkolenia personelu, plan zarządzania podatnościami, plan reagowania na incydenty, plan przywracania,

	plan zarządzania odtwarzaniem po katastrofie.

14) Szkolenia dla pracowników IT.

Analiza i zbieranie logów - szkolenie	
Szkolenie musi być prowadzone przez jednego certyfikowanego inżyniera, posiadającego minimum 4 aktywne certyfikaty producenta oferowanego w postępowaniu rozwiązania do zbierania i przechowywania logów na poziomie: • Certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci(NS) • Certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej(PCS) • Certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa(SO) • Certyfikowany Specjalista w zakresie Dostępu Zero Trust(ZTA)	
Zakres Szkolenia:	1. Podstawowa Konfiguracja Sieciowa: • Skonfigurowanie Adresu IP: o Przydzielanie statycznego adresu IP do urządzenia FAZ. o Konfiguracja adresacji IP w różnych podsieciach. o Rozwiązywanie problemów związanych z konfliktem adresów IP. • Konfiguracja Maski Podsieci: o Zrozumienie i obliczanie maski podsieci. o Implementacja odpowiednich masek podsieci dla różnych segmentów sieci. o Diagnostyka problemów z komunikacją między podsieciami. • Ustawienie Bramy Domyślnej: o Konfiguracja bramy domyślnej dla urządzeń w sieci lokalnej. o Testowanie łączności z bramą domyślną. o Konfiguracja tras statycznych i dynamicznych. • Konfiguracja Serwerów DNS: o Dodawanie i priorytetyzowanie serwerów DNS. o Sprawdzanie poprawności konfiguracji DNS poprzez narzędzia diagnostyczne. o Rozwiązywanie problemów z rozpoznawaniem nazw. 2. Rejestracja Urządzeń: • Dodanie Urządzeń do Analizy: o Procedury dodawania różnych typów urządzeń (routery, switche, serwery). o Automatyczne wykrywanie i ręczne dodawanie urządzeń. o Konfiguracja parametrów urządzeń do optymalizacji logowania. • Weryfikacja Poprawności Rejestracji Urządzeń: o Metody testowania poprawności rejestracji. o Rozwiązywanie problemów z rejestracją. o Monitorowanie stanu połączenia urządzeń. 3. Konfiguracja Logowania: • Skonfigurowanie Urządzeń do Wysyłania Logów do Analizy:

	o Wybór protokołów logowania (Syslog, SNMP, WMI). o Konfiguracja parametrów logowania dla różnych urządzeń. o Zarządzanie buforami logów i zapobieganiem utracie danych. • Weryfikacja Poprawności Konfiguracji Logowania: o Testowanie konfiguracji logowania. o Rozwiązywanie problemów z przesyłaniem logów. o Monitorowanie i raportowanie stanu logowania. 4. Konfiguracja Administratorów: • Utworzenie Kont Administratorów: o Procedury tworzenia kont administracyjnych. o Konfiguracja zabezpieczeń konta (hasła, uwierzytelnianie dwuskładnikowe). o Zarządzanie sesjami i prawami dostępu administratorów. • Ustawienie Odpowiednich Poziomów Uprawnień: o Definiowanie ról i przypisywanie uprawnień. o Zarządzanie politykami dostępu i audytowanie działań administratorów. o Tworzenie i zarządzanie grupami użytkowników. 5. Alerty i Powiadomienia: • Konfiguracja Powiadomień E-mail: o Konfiguracja serwerów SMTP do wysyłania powiadomień. o Personalizacja szablonów e-mailowych dla różnych zdarzeń. o Testowanie i weryfikacja dostarczalności e-maili. • Ustawienie Alertów dla Różnych Zdarzeń Systemowych i Zabezpieczeń: o Tworzenie reguł alertów na podstawie specyficznych zdarzeń. o Konfiguracja eskalacji powiadomień. o Monitorowanie i zarządzanie aktywnymi alertami. 6. Polityki Logowania: • Ustawienie Rodzajów Logów, które Mają Być Przechowywane: o Definiowanie kategorii logów (np. logi ruchu, logi zdarzeń). o Konfiguracja selektywnego logowania w celu optymalizacji wydajności. o Archiwizacja i przenoszenie starych logów do zewnętrznych zasobów. • Konfiguracja Polityk Logowania: o Tworzenie i zarządzanie politykami logowania. o Implementacja reguł dla różnych typów zdarzeń. o Przegląd i aktualizacja polityk na podstawie zmieniających się potrzeb i zagrożeń. 7. Retencja Danych: • Ustawienie Okresów Retencji dla Różnych Typów Logów: o Definiowanie okresów przechowywania dla logów bezpieczeństwa, operacyjnych i innych. o Automatyzacja usuwania starych logów zgodnie z politykami retencji.

	o Audytowanie i raportowanie przestrzegania polityk retencji. • Zarządzanie Miejscem na Dysku Poprzez Polityki Retencji: o Monitorowanie zużycia przestrzeni dyskowej. o Implementacja strategii przechowywania danych w chmurze. o Optymalizacja przestrzeni dyskowej poprzez kompresję i de-duplikację logów. 8. Tworzenie Pulpitów Nawigacyjnych (Dashboards): • Konfiguracja Pulpitów Nawigacyjnych dla Monitorowania w Czasie Rzeczywistym: o Tworzenie i personalizacja interaktywnych dashboardów. o Integracja różnych źródeł danych na pulpitach nawigacyjnych. o Implementacja widgetów i graficznych reprezentacji danych. • Przykłady Zastosowań Pulpitów Nawigacyjnych: o Monitorowanie stanu sieci i urządzeń. o Wizualizacja trendów bezpieczeństwa i wykrytych incydentów. o Analiza wydajności systemów IT. 9. Konfiguracja Raportów: • Tworzenie Szablonów Raportów: o Definiowanie formatów i zawartości raportów. o Personalizacja raportów według potrzeb odbiorców. o Integracja logów z zewnętrznymi narzędziami raportującymi. • Ustalanie Harmonogramów Generowania Raportów: o Automatyzacja cyklicznego generowania raportów. o Dystrybucja raportów do odpowiednich interesariuszy. o Monitorowanie i zarządzanie harmonogramami. 10. Polityki Bezpieczeństwa: • Ustawienie Polityk Zabezpieczeń i Zgodności: o Definiowanie polityk bezpieczeństwa zgodnie z najlepszymi praktykami i regulacjami prawnymi. o Implementacja polityk zgodności (np. RODO, HIPAA). o Audytowanie przestrzegania polityk i zarządzanie wyjątkami. • Konfiguracja Reguł Dostępu i Polityk Zgodności z Przepisami: o Tworzenie i egzekwowanie reguł dostępu do danych i zasobów. o Regularne przeglądy i aktualizacje polityk zgodności. o Implementacja mechanizmów śledzenia i audytu. 11. Testowanie Konfiguracji: • Sprawdzenie Poprawności Konfiguracji Poprzez Testy Funkcjonalne: o Przeprowadzanie testów w celu weryfikacji poprawności konfiguracji. o Analiza wyników testów i identyfikacja problemów.

	o Dokumentacja i wprowadzenie poprawek na podstawie testów. • Symulacje Zdarzeń i Ich Analiza: o Tworzenie scenariuszy testowych dla różnych zdarzeń bezpieczeństwa. o Analiza zachowań systemu podczas symulacji. o Ocena skuteczności konfiguracji zabezpieczeń. 12. Weryfikacja Integracji: • Potwierdzenie, że Wszystkie Urządzenia Są Poprawnie Zintegrowane: o Przegląd listy zintegrowanych urządzeń i ich statusów. o Testy integracyjne dla potwierdzenia poprawności współdziałania. o Rozwiązywanie problemów z integracją i komunikacją. • Weryfikacja, że Urządzenia Wysyłają Logi do Analizy: o Monitorowanie przepływu logów z urządzeń do systemu FAZ. o Weryfikacja poprawności i kompletności danych logów. o Analiza i raportowanie stanu logowania oraz wykrytych anomalii.
Szkolenie z Administracji Active Directory na Microsoft Windows Server	
Opis Szkolenia: **To intensywne szkolenie jest przeznaczone dla administratorów systemów oraz specjalistów IT, którzy chcą zdobyć zaawansowaną wiedzę i umiejętności w zakresie instalacji, konfiguracji i zarządzania usługą Active Directory na platformie Microsoft Windows Server. Uczestnicy nauczą się nie tylko podstawowych operacji, ale także zaawansowanych technik zabezpieczania i optymalizacji środowiska Active Directory. Program obejmuje także dodatkowe moduły dotyczące integracji z serwerami certyfikatów oraz Network Policy Server (RADIUS).**	
Plan Szkolenia:	1. Instalacja Active Directory na Microsoft Windows Server: • Przygotowanie serwera do instalacji roli Active Directory. • Konfiguracja pierwszego kontrolera domeny. • Procedura instalacji usług AD DS. 2. Podstawowe narzędzia do zarządzania Active Directory: • Przegląd narzędzi zarządzania, takich jak Active Directory Users and Computers, Active Directory Sites and Services, Active Directory Domains and Trusts. 3. Zarządzanie użytkownikami: • Dodawanie nowych użytkowników do domeny. • Konfiguracja właściwości obiektów użytkowników. • Zarządzanie grupami użytkowników. • Przyznawanie i zarządzanie uprawnieniami użytkowników. 4. Rola DNS w Active Directory: • Integracja usługi DNS z Active Directory. • Konfiguracja stref DNS i rekordów SRV. 5. Dodawanie komputerów do Active Directory: • Procedura dołączania komputerów do domeny. • Konfiguracja zabezpieczeń komputerów w kontekście domeny. 6. Polityki grup:

	• Stosowanie polityk grup do zabezpieczania i zarządzania środowiskiem Active Directory. • Przekierowanie folderów użytkowników na serwerze plików przy użyciu polityk grup. • Instalacja oprogramowania przy pomocy GPO (Group Policy Objects). 7. Dodawanie kolejnych kontrolerów do domeny Active Directory - redundancja: • Procedura dodawania dodatkowych kontrolerów domeny. • Przenoszenie ról FSMO (Flexible Single Master Operation) pomiędzy kontrolerami. 8. Windows Server Backup: • Konfiguracja i zarządzanie kopiami zapasowymi systemu Active Directory. • Przywracanie danych z kopii zapasowych. 9. Firewall w systemie Windows Server: • Dodawanie i edycja reguł firewalla systemowego Windows Server. • Konfiguracja zabezpieczeń sieciowych na poziomie serwera. 10. (Opcjonalnie) Network Policy Server (RADIUS) i jego integracja z Active Directory: • Konfiguracja Network Policy Server do autoryzacji i uwierzytelniania sieciowego. • Integracja NPS z usługą Active Directory. 11. (Opcjonalnie) Usługi Active Directory Certificate Services: • Przegląd usług AD CS i ich zastosowań. • Procedura instalacji i konfiguracji usług PKI w środowisku Active Directory.
Urządzenie UTM - szkolenie	
Szkolenie musi być prowadzone przez jednego certyfikowanego inżyniera, posiadającego minimum 4 aktywne certyfikaty producenta oferowanego w postępowaniu rozwiązania UTM na poziomie: • Certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci(NS) • Certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej(PCS) • Certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa(SO) • Certyfikowany Specjalista w zakresie Dostępu Zero Trust(ZTA)	
Zakres Szkolenia:	1. Rejestracja Urządzeń oraz Licencji: • Rejestracja Urządzeń w Systemie: o Proces dodawania nowych urządzeń do systemu zarządzania. o Konfiguracja parametrów urządzeń oraz weryfikacja poprawności rejestracji. o Automatyczne wykrywanie urządzeń i integracja z istniejącymi zasobami. • Zarządzanie Licencjami i Subskrypcjami: o Przegląd dostępnych licencji i subskrypcji. o Procedury aktywacji i odnawiania licencji.

	○ Monitorowanie zużycia licencji oraz optymalizacja kosztów. 2. Aktualizacja Oprogramowania i Zmiana Danych Dostępowych: • Procedura Aktualizacji Oprogramowania: ○ Przeprowadzanie aktualizacji firmware'u i oprogramowania urządzeń. ○ Zasady bezpiecznego przeprowadzania aktualizacji (kopie zapasowe, testowanie). ○ Automatyzacja procesu aktualizacji i harmonogramowanie. • Zmiana Danych Dostępowych (Autoryzacja) do Urządzeń: ○ Procedury zmiany haseł i danych autoryzacyjnych. ○ Implementacja polityk zmiany haseł i zarządzania dostępem. ○ Audytowanie i zabezpieczanie danych dostępowych. 3. Konfiguracja Metod Dostępu i Segmentacji Sieci: 1. Konfiguracja Metod Dostępu do Urządzeń: ○ Konfiguracja Dostępu SSH i HTTPS: ▪ Implementacja i konfiguracja bezpiecznego dostępu do urządzeń. ▪ Zarządzanie certyfikatami SSL/TLS. ○ Wdrożenie Dwuetapowej Autoryzacji (2FA): ▪ Implementacja 2FA dla zwiększenia bezpieczeństwa dostępu. ▪ Konfiguracja aplikacji autoryzujących i tokenów sprzętowych. 2. Konfiguracja Łącz Dostępowych do Internetu i Redundancji: ○ Ustawienie Podstawowych Łącz Internetowych: ▪ Konfiguracja głównych połączeń internetowych. ▪ Monitorowanie i optymalizacja wydajności łączy. ○ Konfiguracja Łącz Zapasowych i Redundancji (WAN): ▪ Implementacja zapasowych łączy internetowych. ▪ Konfiguracja mechanizmów przełączania awaryjnego i load balancingu. 3. Segmentacja Sieci LAN: ○ Konfiguracja Interfejsów Sieciowych: ▪ Ustawienia interfejsów fizycznych i logicznych. ▪ Optymalizacja parametrów interfejsów dla różnych zastosowań. ○ Konfiguracja VLAN i Polityk Dostępu do Podsieci/VLAN: ▪ Tworzenie i zarządzanie VLANami. ▪ Implementacja polityk bezpieczeństwa dla poszczególnych VLANów. 4. Zarządzanie Siecią i Polityki Bezpieczeństwa: 1. Uruchomienie Serwerów DHCP: ○ Konfiguracja Serwerów DHCP na Poszczególnych Podsieciach/VLAN: ▪ Ustawienia serwerów DHCP dla dynamicznego przydzielania adresów IP.

	▪ Zarządzanie pulami adresów i rezerwacjami. 2. Konfiguracja Routingu i Agregacji Portów: o Ustawienia Routingu Statycznego i Dynamicznego: ▪ Konfiguracja tras statycznych i protokołów routingu dynamicznego (OSPF, BGP). ▪ Optymalizacja trasowania i zarządzanie tablicami routingu. o Konfiguracja Agregacji Portów dla Zwiększenia Przepustowości: ▪ Implementacja agregacji portów (LACP). ▪ Balansowanie obciążenia i redundancja portów. 3. Polityki Bezpieczeństwa: o Filtrowanie i Blokowanie Treści oraz Aplikacji Internetowych: ▪ Konfiguracja filtrów treści i aplikacji. ▪ Zarządzanie czarnymi i białymi listami. o Konfiguracja Antywirusa, Filtrów DNS, IPS i DLP: ▪ Implementacja zabezpieczeń antywirusowych i systemów wykrywania intruzji (IPS). ▪ Konfiguracja filtrów DNS i polityk zapobiegania wyciekom danych (DLP). 5. Integracja i Zarządzanie Systemem: 1. Integracja z Domena: o Konfiguracja Urządzeń do Współpracy z Domena: ▪ Procedury integracji z domeną Active Directory. ▪ Zarządzanie kontami i politykami bezpieczeństwa domeny. 2. Konfiguracja SNMP: o Ustawienia SNMP do Monitorowania Sieci: ▪ Konfiguracja protokołu SNMP dla monitorowania i zarządzania urządzeniami sieciowymi. ▪ Implementacja pułapek SNMP i zbieranie danych z urządzeń. 6. Logowanie, Kopie Zapasowe i VPN: 1. Konfiguracja Procesu Logowania: o Konfiguracja Zawartości Logów i Okresu Przechowywania: ▪ Definiowanie typów logów, które mają być przechowywane. ▪ Ustalanie okresów retencji logów i zarządzanie przestrzenią dyskową. 2. Wykonanie Kopii Zapasowej Ustawień Urządzeń: o Procedury Tworzenia Kopii Zapasowych i Przywracania Ustawień: ▪ Automatyzacja tworzenia kopii zapasowych ustawień urządzeń. ▪ Procedury przywracania ustawień z kopii zapasowych. 3. Konfiguracja Tuneli VPN IPsec / SSL: o Konfiguracja Tuneli VPN Typu IPsec i SSL:

	▪ Tworzenie i zarządzanie tunelami VPN dla bezpiecznej komunikacji. ▪ Konfiguracja polityk bezpieczeństwa VPN i zarządzanie certyfikatami.
Szkolenie z Administracji i Zarządzania Systemami NAS	
To zaawansowane szkolenie jest skierowane do administratorów IT oraz specjalistów zajmujących się zarządzaniem systemami backupu i NAS (Network Attached Storage) w organizacjach. Uczestnicy zdobędą kompleksową wiedzę na temat instalacji, konfiguracji oraz zaawansowanych funkcji oferowanych przez oprogramowanie do backupu i systemy NAS. Program obejmuje szeroki zakres tematów, w tym: • Konfigurację, zarządzanie i zabezpieczanie systemów NAS, od podstawowych funkcji sprzętowych po zaawansowane techniki wirtualizacji i zabezpieczeń. • Ochronę przed atakami ransomware i przywracanie systemów przy użyciu technologii Disaster Recovery. • Najlepsze praktyki oraz praktyczne umiejętności, które uczestnicy będą mogli zastosować w swoich organizacjach. Szkolenie ma na celu pogłębienie wiedzy i umiejętności uczestników, umożliwiając im skuteczne zarządzanie i zabezpieczanie kluczowych zasobów IT w swojej organizacji.	
Plan Szkolenia:	1. Wprowadzenie: • Wprowadzenie do szkolenia, cele i oczekiwania. • Przegląd agendy i struktury szkolenia. • Omówienie korzyści z zastosowania systemów NAS w przedsiębiorstwie. 2. Przegląd Produktów NAS: • Omówienie różnych modeli systemów NAS i ich zastosowań. • Podstawowe funkcje i możliwości sprzętowe i programowe. • Przykłady wdrożeń systemów NAS w różnych branżach. 3. Podstawowe Informacje o Możliwościach Sprzętowych i Programowych: • Szczegółowy przegląd architektury sprzętowej. • Wprowadzenie do oprogramowania systemowego i jego funkcji. • Zarządzanie zasobami sprzętowymi i programowymi w systemach NAS. 4. Zarządzanie Dyskami i Konfiguracja Przestrzeni: • Podstawy zarządzania dyskami w systemach NAS. • Procedury instalacji i konfiguracji dysków twardych. • Monitorowanie stanu dysków i rozwiązywanie problemów. 5. Architektura Przestrzeni Dyskowej: • Szczegółowe omówienie architektury pamięci masowej w systemach NAS.

	• Koncepcje i komponenty systemów przechowywania danych. • Zarządzanie przestrzenią dyskową i optymalizacja wydajności. 6. Dobór Dysków Twardych i Możliwości Konfiguracji: • Kryteria doboru dysków twardych do systemów NAS. • Przegląd różnych typów dysków (HDD, SSD) i ich zastosowań. • Konfiguracja RAID i innych technologii ochrony danych. 7. Konfiguracja Puli Pamięci z Technologią Automatycznego Tieringu: • Wprowadzenie do technologii automatycznego tieringu danych. • Konfiguracja puli pamięci z różnymi poziomami przechowywania. • Zarządzanie danymi w oparciu o ich częstotliwość dostępu. 8. Konfiguracja Woluminów: • Tworzenie i zarządzanie woluminami na urządzeniach NAS. • Optymalizacja przestrzeni dyskowej i zarządzanie zasobami. • Monitorowanie i rozszerzanie woluminów. 9. Konfiguracja iSCSI LUN: • Tworzenie i zarządzanie jednostkami logicznymi (LUN). • Integracja systemów NAS z serwerami i innymi urządzeniami. • Zarządzanie dostępem i wydajnością iSCSI LUN. 10. Konfiguracja SSD Cache: • Implementacja i zarządzanie pamięcią cache SSD. • Optymalizacja wydajności systemu poprzez przyspieszenie operacji odczytu/zapisu. • Monitorowanie i zarządzanie zasobami cache. 11. Wirtualne Pamięci i Chmura: • Konfiguracja wirtualnych jednostek pamięci (VJBOD). • Integracja z usługami chmurowymi i zdalnymi zasobami. • Zarządzanie danymi w chmurze i synchronizacja z lokalnymi zasobami. 12. CacheMount: • Wprowadzenie do technologii CacheMount. • Konfiguracja i zarządzanie dostępem do zewnętrznych zasobów. • Optymalizacja wydajności poprzez cache'owanie danych. 13. Przechowywanie Danych: • Metody i strategie przechowywania danych. • Zarządzanie przestrzenią dyskową i optymalizacja jej wykorzystania.

	• Wdrażanie polityk przechowywania i archiwizacji danych. 14. Zarządzanie Uprawnieniami: • Konfiguracja uprawnień użytkowników i grup. • Zarządzanie dostępem do zasobów i monitorowanie aktywności. • Implementacja polityk bezpieczeństwa dostępu. 15. Udziały Sieciowe: • Tworzenie i zarządzanie udziałami sieciowymi. • Konfiguracja dostępu i uprawnień do udziałów sieciowych. • Monitorowanie i zarządzanie udostępnionymi zasobami. 16. Backup i Replikacja: • Strategie backupu i replikacji danych. • Konfiguracja i zarządzanie kopiami zapasowymi. • Wdrażanie polityk backupu i odzyskiwania danych. 17. Narzędzie do Hybrydowego Backup i Synchronizacji: • Wprowadzenie do narzędzia hybrydowego backupu i synchronizacji. • Konfiguracja i zarządzanie synchronizacją i backupem danych. • Optymalizacja procesów backupu i synchronizacji. 18. Deduplikacja: • Techniki deduplikacji danych. • Konfiguracja i zarządzanie deduplikacją. • Optymalizacja przestrzeni dyskowej poprzez deduplikację. 19. Wirtualizacja: • Podstawy wirtualizacji na systemach NAS. • Tworzenie i zarządzanie maszynami wirtualnymi. • Integracja wirtualizacji z innymi zasobami IT. 20. Konfiguracja Sieci Wirtualnej: • Tworzenie i zarządzanie sieciami wirtualnymi. • Integracja z fizycznymi sieciami i systemami. • Optymalizacja wydajności sieci wirtualnych. 21. Wirtualizacja na NAS: • Implementacja rozwiązań wirtualizacyjnych na systemach NAS. • Zarządzanie zasobami wirtualnymi. • Monitorowanie wydajności i rozwiązywanie problemów.

	22. Kontenery: • Wprowadzenie do technologii kontenerów. • Tworzenie i zarządzanie kontenerami na systemach NAS. • Integracja kontenerów z innymi zasobami i usługami. 23. Zabezpieczenie Systemów NAS: • Metody zabezpieczania systemów NAS. • Implementacja polityk bezpieczeństwa i zarządzanie ryzykiem. • Monitorowanie i reagowanie na zagrożenia. 24. Narzędzie do Analizy Bezpieczeństwa: • Wprowadzenie do narzędzia analizy bezpieczeństwa. • Konfiguracja i zarządzanie bezpieczeństwem systemu. • Wdrażanie rekomendacji i polityk bezpieczeństwa. 25. Zabezpieczenie przed Atakami Brute Force: • Metody ochrony przed atakami brute force. • Konfiguracja zabezpieczeń i polityk dostępu. • Monitorowanie i reagowanie na próby ataków. 26. Konfiguracja Antywirusa: • Implementacja i zarządzanie oprogramowaniem antywirusowym. • Skanowanie i ochrona systemu przed zagrożeniami. • Automatyzacja procesów skanowania i aktualizacji. 27. Szyfrowanie Dysków i Katalogów: • Techniki szyfrowania danych. • Konfiguracja szyfrowania na poziomie dysków i katalogów. • Zarządzanie kluczami szyfrowania i politykami dostępu. 28. Zarządzanie Hasłami Użytkowników: • Polityki zarządzania hasłami. • Implementacja i zarządzanie politykami bezpieczeństwa haseł. • Monitorowanie i audytowanie zmian haseł i dostępu. • Opis Szkolenia: 29. Wprowadzenie do Oprogramowania do Backupu: • Przegląd funkcji i możliwości systemu backupowego. • Cele szkolenia i oczekiwania uczestników. 30. Dostępne rozwiązania i ich architektura: • Omówienie różnych rozwiązań backupowych oferowanych przez oprogramowanie do backupu.

	• Architektura systemowa i wymagania techniczne. 31. Instalacja i konfiguracja serwera backupu: • Procedura instalacji serwera backupowego. • Konfiguracja podstawowych ustawień i integracja z istniejącą infrastrukturą IT. 32. Organizacja struktury grup oraz użytkowników w systemie: • Tworzenie i zarządzanie grupami użytkowników w panelu administracyjnym oprogramowania do backupu. • Przypisywanie uprawnień i dostosowywanie poziomów dostępu. 33. Przypisywanie urządzeń i definiowanie polityk backupu: • Konfiguracja urządzeń do backupu. • Definiowanie polityk backupu plików i aplikacji. 34. Przegląd platformy Oprogramowania do Backupu: • Omówienie interfejsu użytkownika i funkcji panelu administracyjnego oprogramowania do backupu. • Praktyczne przykłady korzystania z panelu kontrolnego. 35. Poziom I - backup plikowy: • Konfiguracja i zarządzanie backupem plików. • Strategie backupu plikowego i przywracania danych. 36. Poziom II - Smart Image Backup: • Wprowadzenie do Smart Image Backup. • Konfiguracja i optymalizacja backupu systemów operacyjnych. 37. Poziom III - bazy danych oraz wirtualizacja: • Backup i ochrona baz danych. • Optymalizacja backupu maszyn wirtualnych. 38. Atak ransomware na żywo oraz technologie Disaster Recovery: • Demonstracja ataku ransomware i skutków dla danych. • Strategie i technologie Disaster Recovery w oprogramowaniu do backupu.

15) Szkolenia pracowników w zakresie cyberbezpieczeństwa.

Szkolenia stacjonarne	ZAKRES usługi przeprowadzenia szkoleń z zakresu cyberbezpieczeństwa SZKOLENIE obejmujące swoim zakresem następujące zagadnienia: Data Leak – czym jest i jakie zagrożenia niesie. Polityka haseł – praktyczne podejście i narzędzia wspomagające. Socjotechniki – podstawowe definicje i przykłady użycia. Phishing / Spoofing – nigdy nie wiesz kto jest po drugiej stronie. Vhishing / ID Call Hijacking – telefony też nie są w pełni bezpieczne. Metadane – czyli dane o danych. Web Archive – Internet nie zapomina. Pliki Cookies – czym są popularne „ciasteczka”. Zagrożenia związane z nieznanym sprzętem – jak nieznany pendrive może zaszkodzić całej instytucji. Ataki Bruteforce / Ataki Słownikowe – podstawowe metody łamania haseł. Spear Phishing – wszystko co „powiesz” (w sieci) może zostać użyte przeciwko Tobie. Sposób organizacji szkolenia: Tryb wykonania szkolenia: stacjonarne Czas trwania szkolenia: 2 godziny Liczba pracowników do przeszkolenia: 160 osób Ilość grup szkoleniowych: 4 Liczba dni szkoleniowych: 2 dni
Platforma eLearningowa	Przedmiotem zamówienia jest kompleksowa usługa „Podnoszenia Świadomości Bezpieczeństwa” (Security Awareness), umożliwiająca przeprowadzenie kampanii edukacyjnej z zakresu podstaw bezpieczeństwa w internecie. Dedykowana jest użytkownikom Zamawiającego i świadczona przez okres 6 miesięcy. Usługa musi zawierać: 1. Platformę szkoleniową zawierającą minimum 50 szkoleń, dostępnych w języku polskim (oraz w jęz. angielskim, niemieckim, hiszpańskim, czeskim, słowackim, serbskim, chorwackim i włoskim), w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego. a) Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu: ✓ Podstawy bezpiecznego internetu ✓ Bezpieczeństwo poczty ✓ Załączniki w poczcie elektronicznej ✓ Phishing ✓ Spyware/malware ✓ Bezpieczeństwo danych osobowych RODO/GDRP ✓ Bezpieczne hasła ✓ Menedżery haseł ✓ Bezpieczeństwo urządzeń mobilnych ✓ Uwierzytelnianie wieloskładnikowe (MFA) ✓ Bezpieczna praca zdalna ✓ Bezpieczna praca w biurze ✓ Sieci społeczne ✓ Socjotechnika stosowana ✓ Zakupy w internecie

	b) Użytkownicy powinni być podzieleni na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe. c) Łączny czas trwania wszystkich materiałów szkoleniowych powinien wynosić co najmniej 8 godzin. 2. Dedykowaną platformę phishingową pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail: a) z linkiem prowadzącym do stronnym internetowej, b) z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji, c) z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod, d) z załącznikiem w postaci dokumentu Word lub Excel zawierającym potencjalnie niebezpieczny kod. W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń. 3. dedykowaną platformę dostarczającą raporty obejmujące minimum: a) status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów, b) status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zwierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, jaka była platforma z jakiej wykonał tę akację oraz szczegółowe daty wykonania tych operacji. W ramach świadczonej usługi usługodawca musi: - przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników, - zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi, - zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail, - dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe, - wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń lub liczby użytkowników (nie więcej niż 10 zmian w okresie trwania usługi). Wymagania dodatkowe: Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi. *Wszystkie moduły*

	(platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta. Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.
PRZEDMIOTOWE ŚRODKI DOWODOWE	Do oferty należy załączyć oświadczenie usługodawcy o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001.

16) Wdrożenia

Nazwa	**Minimalne wymagania dla usługi**
Typ	Usługi informatyczne - Wdrożenie nowego sprzętu
Wdrożenie sprzętu serwerowego opisanego w punkcie 1. “Serwer”	Zamawiający w ramach dostawy wymaga usługi wdrożenia dostarczanych rozwiązań. Zamawiający wymaga, aby w ramach wdrożenia zostały wykonane prace w minimalnym zakresie: • Serwer musi zostać dostarczony i fizycznie zamontowany w miejscu wskazanym przez zamawiającego. • Dostarczone oprogramowanie serwerowe musi zostać zaktualizowane do najnowszej wersji na dzień wdrożenia. • Serwer musi zostać zamontowany tak, aby ułożenie przewodów w jak najmniejszym stopniu zakłócało cyrkulację powietrze. Przewody muszą zostać opisane. • Na dostarczanym serwerze i na serwerze Zamawiającego muszą zostać zainstalowane maksymalnie cztery instancję systemów zaoferowanych w ramach postępowania • Serwery fizyczne jak i serwery wirtualne muszą zostać zaadresowane zgodnie z wymaganiami przekazanymi w czasie wdrożenia. • Dla serwerów wirtualnych muszą zostać stworzone co najmniej 3 przełączniki wirtualne. • Na jednej z maszyn musi zostać uruchomiona usługa katalogowa. Do usługi katalogowej musi zostać podłączony dostarczany sprzęt wraz z maksymalnie 5 urządzeniami typu komputer osobisty w celach instruktażowych. W usłudze katalogowej muszą zostać skonfigurowane podstawowe polityki bezpieczeństwa i maksymalnie 5 dedykowanych w tym dotyczące zdalnej instalacji oprogramowania. Na jednej z maszyn wirtualnej musi zostać uruchomiona baza danych Microsoft SQL Server oraz osobno baza FireBird. W ramach wdrożenia muszą zostać przeniesione pokazowo minimum 2 bazy każdego silnika

	bazodanowego.
Wdrożenie oprogramowania do monitorowania infrastruktury informatycznej opisane w punkcie 7. „Analizer Logów”	Instalacja oprogramowania do monitorowania infrastruktury informatycznej wraz z wdrożeniem agentów zdalnego zarządzania za pomocą wdrożonej usługi katalogowej.
Wdrożenie oprogramowania do wykonywania kopii zapasowych opisanego w punkcie 3. ”Oprogramowanie do wykonywania kopii bezpieczeństwa”	Na jednej z maszyn wirtualnych musi zostać zainstalowane oprogramowanie do backupu wraz z podłączeniem do niego serwerów i instruktażowo 2 urządzeń typu komputer osobisty. Muszą zostać skonfigurowane polityki backupu.
Wdrożenie oprogramowania DLP (Data Leak Prevention) opisanego w punkcie 9. „System DLP”	· Instalacja oprogramowania DLP · Instalacja konsoli zarządzającej · Przeprowadzenie logowania do konsoli zarządzającej · Konfiguracja SMTP · Podłączenie do infrastruktury posiadanej przez Zamawiającego (Active Directory) · Wygenerowanie agenta rozwiązania DLP oraz przeprowadzenie instalacji na środowiskach testowych wybranych przed wdrożeniem · Przypisanie licencji · Konfiguracja raportowania i monitorowania · Utworzenie stref bezpiecznych i niebezpiecznych · Instalacja klienta na stacjach z zainstalowanym agentem · Utworzenie reguł DLP wcześniej skonsultowanych z Zamawiającym · Wykonanie testów
Wdrożenie urządzeń typu UTM opisanych w punktach 4 oraz 5. „UTM wraz z serwisem”	Wdrożenie musi być wykonane przy asyście pracownika Urzędu Miejskiego w Siechnicach. Konfiguracja Metod Dostępu do Urządzeń · Konfiguracja Łącz Dostępowych do Internetu i Redundancji · Uruchomienie Serwerów DHCP · Konfiguracja Routingu i Agregacji Portów · Filtrowanie i Blokowanie Treści oraz Aplikacji Internetowych · Konfiguracja Antywirusa, Filtrów DNS, IPS i DLP · Konfiguracja Urządzeń do Współpracy z Domeną · Wykonanie Kopii Zapasowej Ustawień Urządzeń · Zarządzanie Licencjami i Subskrypcjami (aktywacja licencji) Wdrożenie musi być prowadzone przez jednego certyfikowanego inżyniera, posiadającego minimum 4 aktywne certyfikaty producenta oferowanego w postępowaniu rozwiązania UTM na poziomie: • Certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci(NS) • Certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej(PCS) • Certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa(SO) • Certyfikowany Specjalista w zakresie Dostępu Zero Trust(ZTA)
Wdrożenie systemu EDR, XDR zintegrowanego z systemem antywirusowym opisanym w punkcie 8. „system EDR, XDR zintegrowanego z systemem	• Rejestracja licencji na koncie Eset Business Account oraz uruchomienie konsoli PROTECT; • Przygotowanie paczek instalacyjnych oprogramowania klienckiego wraz z agentem dla systemów Windows;

antywirusowym”	• Wdrożenie agenta; • Migracja danych z starej konsoli ESET PROTECT; • Przygotowanie polityki: dla agenta, działu IT, ogólnej dla organizacji; • Utworzenie i uruchomienie zadania instalacji produktu zabezpieczającego Eset Endpoint Security; • Konfiguracja polityki szyfrowania dysków; • Uruchomienie szyrowania dysków na wskazanych hostach; • Konfiguracja polityki dla Sandboxa w chmurze; • Uruchomienie konsoli Eset Inspect; • Włączenie domyślnych reguł zgodnie z założeniami administratora; • Uruchomienie na wskazanych urządzeniach funkcji EDR; • Uruchomienie innych modułów ochronnych zawartych w pakiecie.
	•
Dokumentacja powdrożeniowa	Wszelkie prace związane z usługą wdrożenia muszą zostać przedstawione w dokumentacji powdrożeniowej posiadającej w swym zakresie wszystkie niezbędne i szczegółowe z punktu widzenia wdrożenia skonfigurowane opcje.

Wymagania ogólne dotyczące identyfikacji oferowanego sprzętu oraz zasad równoważności.

1. Dla jednoznacznej identyfikacji oferowanych rozwiązań należy podać co najmniej nazwę producenta, a także nazwę i model oferowanego produktu lub jego oznaczenie kodowe wg. producenta. Zamawiający wymaga określenia oferowanych produktów i faktycznych parametrów, o których mowa w powyższym opisie, w taki sposób, by oceniający byli w stanie stwierdzić, czy zaoferowany rozwiązanie spełnia wymagania specyfikacji. Przedmiotowe informacje są składane na potwierdzenie, iż oferowane rozwiązania spełniają wymagania Zamawiającego. Ciężar wykazania spełnienia przez oferowane rozwiązania wymogów określonych przez Zamawiającego w specyfikacji spoczywa na składającym ofertę.

2. O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.

3. W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.

4. W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.

5. Pod pojęciem rozwiązań równoważnych, o ile nie dokonano doprecyzowania w danym zakresie, Zamawiający rozumie taki sprzęt i oprogramowanie, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w Opisie Przedmiotu Zamówienia.

6. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

7. Ciężar udowodnienia równoważności w stosunku do wymogów określonych przez Zamawiającego spoczywa na składającym ofertę. W takim przypadku Wykonawca musi przedłożyć odpowiednie dokumenty, opisujące parametry techniczne, wymagane prawem certyfikaty i inne dokumenty, dopuszczające dane produkty do użytkowania oraz pozwalające jednoznacznie określić, że są równoważne.

8. Wykonawca dostarczy harmonogram dostaw, wdrożeń oraz szkoleń z podziałem na poszczególne elementy, które zostaną uzgodnione z Zamawiającym.