Załącznik numer 6 – Szczegółowy opis przedmiotu zamówienia

Cześć 1 : Zapora antyspamowa

Parametr	Wymagania
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 ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure. 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	System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.
Ogólne funkcje systemu ochrony poczty	Wsparcie dla co najmniej 20 domen pocztowych
	System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
	Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
	Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).

	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.
	Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
	Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
	Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
	Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
	Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
	Dostęp do kwarantanny użytkownika możliwy poprzez WebMail. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
	1. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki. 2. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
	3. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
	4. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
	5. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
	Skanowanie antywirusowe wiadomości SMTP
	Kwarantannę dla zainfekowanych plików.
	Skanowanie załączników skompresowanych.
	Definiowanie komunikatów powiadomień w języku polskim.

Kontrola antywirusowa i ochrona przed malware	
	Blokowanie załączników w oparciu o typ pliku.
	Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
	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.
	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.
	Ochronę typu wirus outbrake.
Kontrola antyspamowa	Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
	Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
	Szczegółowa kontrola nagłówka wiadomości.
	Analiza Heurystyczna.
	Współpraca z zewnętrznymi serwerami RBL, SURBL.
	Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
	Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
	Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
	Kontrola w oparciu o Greylisting oraz SPF.
	Filtrowanie treści wiadomości i załączników.
	Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.

	Ochrona typu outbrake. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
	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	Ochrona przed atakami na adres odbiorcy (m.in. email bombing)
	Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
	Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
	Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
	Weryfikacja poprawności adresu e-mail nadawcy.
Funkcje logowania i raportowania	Logowanie do zewnętrznego serwera SYSLOG.
	Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
	Logowanie informacji na temat spamu oraz niedozwolonych załączników.
	Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
	Możliwość analizy przebiegu sesji SMTP.
	Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
	Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
	Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
Funkcje pracy w trybie wysokiej dostępności (HA)	Konfigurację HA w każdym z trybów: gateway, transparent.
	Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
	Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
	Monitorowanie stanu pracy klastra.

Aktualizacje sygnatur, dostęp do bazy spamu	Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
	Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
Zarządzanie	System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
	Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
	Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.

Certyfikaty	Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji : VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.
Serwisy i licencje	System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake na okres 12 miesięcy.
Gwarancja oraz wsparcie	System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
Opisy do wymagań ogólnych	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.
	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
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 1 sztuki

Cześć 2 : Serwer NAS

Parametr	Wymagania
Procesor	Procesor 64 bit x86 o takowaniu nie mniejszym niż 2.2 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 16GB DDR4
Pamieć RAM liczba slotów	Minimum 2 sloty
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 64GB
Pamięć Flash	Nie mniej niż 5 GB
Liczba zatok na dyski twarde	Minimum 16
Obsugiwane dyski twarde	3.5" oraz 2.5" SATA oraz 2.5" SATA SSD
Pojemność dysków twardych	do 24TB
Zainstalowane dyski twarde	16x 20TB, 7200RPM, min 256GB Cache – model dysku musi się znajdować na liscie dysków kompatybilnych z danym modelem urządzenia
Możliwość podłączenia modułu rozszerzającego	Tak, minimum 9, może wymagać dodatkowej karty rozszerzeń
Porty LAN 2,5 GbE	Minimum 2 RJ-45
Porty SFP+ 10Gbe	Minimum 2 SFP+ wraz z wkładkami typu Multi Mode
Diody LED	Minimum Status, LAN, HDD,
Porty USB 3.2 Gen1	Minimum 1
Porty USB 3.2 Gen2 (10 Gb/s)	Minimum 2 Typ C i 1 Typ A
Port PCiE	Tak, minimum 2 Gen3x4 (min 1 wolny port)
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 3U
Dopuszczalna temperatura pracy	od 0 do 40˚C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Zasilacz redundatny 2 x 550 W, 100-240 V

Specyfikacja oprogramowania	
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie wolumenów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, 50, 60, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business, Box

Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Możliwość aktualizacji oprogramowania Ustawienia: Back up, przywracania, resetowania systemu
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker

Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja	3 lata
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 1 sztuki

Cześć 3 : Oprogramowanie do backupu

Wymagania ogólne	Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
	Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
	Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.5.x - 6.7.x, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4 lub nowszy oraz Proxmox VE 8.2 lub nowszy.
	Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
Całkowite koszty posiadania	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
	Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków

	Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
	Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
	Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
	Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
	Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
	Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
	Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
	Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
	Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
	Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
	Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji

	Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
	Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
	Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
	Oprogramowanie musi wymagać autoryzacji dwuch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora)
	Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS)
	Oprogramowanie musi posiadać integracje z systemami typu SIEM
	Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.
Wymagania RPO	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
	Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
	Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru
	Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
	Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
	Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).

	Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
	Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
	Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
	Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
	Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
	Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
	Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
	Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
	Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
Wymagania RTO	Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
	Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
	Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się

	mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
	Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
	Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
	Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
	Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
	Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
	Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
	Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
	Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.

	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
	Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
	Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
	Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
	Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji
	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2
	Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Ograniczenie ryzyka	Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
	Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.

	Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
	Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
	Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware
	Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania
	Oprogramowanie, bazując na wyuczonynym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków
	Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
	Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR
Środowiska fizyczne	Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
	Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
	Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, Rocky Linux, AlmaLinux
	Rozwiązanie musi wspierać system operacyjny macOS
	Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
	Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
	Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster

	Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
	Rozwiązanie musi wspierać backup podłączonych dysków USB
	Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
	Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
	Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
	Rozwiązanie musi wspierać kontrolę pasma sieciowego
	Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
	Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
	Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
	Rozwiązanie musi wspierać technologię BitLocker
	Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
	Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
	Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
	Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
	Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform

	Rozwiązanie musi wspierać szyfrowanie
	Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
	Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
	Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
Monitoring	System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
	System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
	System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
	System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
	System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
	System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
	System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
	System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
	System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów

	System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
	System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
	System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
	System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
	System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
	System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
	System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
	System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.6
Raportowanie	System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
	System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
	System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
	System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
	System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
	System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc

	System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
	System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
	System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
	System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
	System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
	System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
	System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
	System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.
	System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
	System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
	System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

Cześć 4 : Przełącznik sieciowy

Parametr	Wymagania
Obudowa	Do montażu w szafie Rack 19", o wysokości nie wiecej niż 1U, wraz z kompletem odpowiednich szyn, wyposażona w zintegrowany zasilacz HotPlug, możliwość instalacji drugiego redundantnego zasilacza.
Porty	Minimum 48 portów Gigabit Ethernet w standardzie Base-T POE+, minimum 4 zintegrowane porty 10Gb Ethernet SFP+, możliwość wyposażenia w minimum 2 porty do łączenia przełączników w stos, minimum 1 port USB do konfiguracji przełącznika, 1 port RJ45 do portu konsoli wraz z odpowiednim kablem RJ45-RS232.
Wydajność przełacznika	- Minimum 16000 adresów MAC - switch fabric capacity min. 176Gbps w trybie full-duplex - forwarding rate min. 130Mpps - pamięć flash min. 2GB - bufor pamięci dla pakietów minimum 2MB - pamięć RAM minimum 2GB - przepustowość stackowania min. 80Gbps - możliwość połączenia w stos do 8 urządzeń tego samego typu - Budżet PoE 740W dla jednego zasilacza, 1440W dla dwóch zasilaczy
Funkcjonalność warstwy II	- obsługa minimum 4000 wirtualnych sieci - obsługa minimum 1500 wpisów ACL - wsparcie dla agregacji LACP (802.3ad) - obsługa 8 grup LACP i 8 portów fizycznych per grupa - obsługa technologii port mirroring (SPAN) oraz remote port mirroring (RSPAN) - obsługa funkcjonalności Voice VLAN
Funkcjonalność warstwy III	- obsługa minimum 3000 wpisów routingu IPv4 - obsługa minimum 1500 wpisów routingu IPv4 - obsługa routingu statycznego oraz RIPv2 - obługa PBR
Zgodność z protokołami / standardami	IEEE 802.1s IEEE 802.w IEEE 802.1x IEEE 802.1Q IEEE 802.3af IEEE 802.3at IEEE 802.3x IEEE 802.1D IEEE 802.1W IEEE 802.1S IEEE 802.1p IEEE 802.3 IEEE 802.3ad IEEE 802.3u IEEE 802.3ab IEEE 802.3z

	IEEE 802.1AE MACsec Jumbo frames – 9198 bajtów RADIUS SSHv2 RMON I oraz II Netflow / Sflow VRRP PVLAN (private VLAN) SNMPv1, v2c, v3 2011 IP MIB 2012 TCP MIB 2013 UDP MIB 2819 RMON MIB LLDP MIB Zgodność z NETCONF, RESTCONF
Zarządzanie siecią i bezpieczeństwo	Sprzęt musi obsługiwać zarządzanie poprzez narzędzie do centralnego monitorowania i zarządzania oferowane przez producenta urządzenia. Zarządzanie z CLI
Warunki pracy	- temperatura pracy w zakresie od 0 do 40 stopni Celsjusza - wilgotność dla trybu pracy 10% do 85% bez kondensacji
Licencje	Dostawca dostarczy niezbędne licencje do uruchomienia protokołu IEEE 802.1ae – MacSec Dostarczana licencja musi funkcjonować z urządzeniami posiadanymi przez Zamawiającego: EX3400-48P w ramach mechanizmu MACsec
Gwarancja	- Stan fabrycznie nowy. - 5 lat gwarancji producenta lub dostawcy na dostarczone urządzenie. - 1 rok dostępu do aktualizacji oprogramowania dla urządzenia wraz z dostępem do pomocy technicznej producenta z możliwością przedłużenia.
Kompatybilność	- Urządzenie musi umożliwiać stackowanie z innymi urządzeniami takiego samego typu w ilości nie mniejszej niż 10 sztuk. Stackowanie powinno być możliwe przy wykorzystaniu standardowych portów typu uplink. Dopuszczalne są rozwiązania, gdzie stackowanie jest wbudowaną funkcjonalnością, oraz takie gdzie stackowanie wymaga zakupu dodatkowej licencji. Jeśli dla realizacji tej funkcji wymagana jest licencja to Zamawiający nie wymaga jej dostarczenia w ramach niniejszego postępowania. Urządzenie musi stackować się z urządzeniami posiadanymi przez Zamawiającego: EX3400-48P w ramach mechanizmu Virtual Chassis.
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 2 sztuk

Cześć 5 : Autentykator MFA

Parametr	Wymagania
Architektura	1. Konsola zarządzania systemem oraz panel administracyjny znajdują się w chmurze. 2. Wszystkie komponenty rozwiązania oraz zbierane dane nie opuszczają terytorium UE, a retencja danych to jeden rok. 3. Rozwiązanie zbiera minimalną ilość informacji o użytkowniku pozwalającą na świadczenie usługi, a szczegółowe wytyczne w kwestii danych przetwarzanych przez dostawcę są udostępnione w formie oficjalnego dokumentu. 4. Ze względów bezpieczeństwa system rozdziela pierwszy oraz drugi składnik uwierzytelnienia w ten sposób, że: a) pierwszy składnik uwierzytelnienia przetrzymywany jest w ramach wyodrębnionego systemu trzeciego IdP tzw. (Identity Provider) b) drugi składnik uwierzytelnienia przetrzymywany jest w ramach osobnego i niezależnego systemu dostarczanego z chmury c) kompromitacja systemu przetrzymującego pierwszy składnik uwierzytelnienia nie powoduje kompromitacji systemu przetrzymującego drugi składnik uwierzytelnienia d) kompromitacja systemu przetrzymującego drugi składnik uwierzytelnienia nie powoduje kompromitacji systemu przetrzymującego pierwszy składnik uwierzytelnienia 5. Komponent IdP umożliwia zarówno instalację lokalną (on premise) jak i w środowisku chmurowym. 6. System chmurowy odpowiedzialny za drugi składnik uwierzytelniania zbudowany jest w oparciu o odporną na awarię architekturę wysokiej klasy oraz charakteryzuje się wysoką dostępność infrastruktury.
Funkcjonalność systemu	7. System umożliwia kontrolę dostępu do aplikacji chmurowych lub znajdujących się w sieci lokalnej z wykorzystaniem drugiego (dodatkowego) składnika uwierzytelnienia w postaci: a) instrukcji potwierdzenia logowania wysyłanej na urządzenie mobilne w ramach dedykowanej aplikacji instalowanej na urządzeniu mobilnym wspierającej systemy iOS i Android, tzw. powiadomienie “push” na urządzeniu mobilnym b) SMS c) połączenia telefonicznego d) kluczyka USB U2F e) tokenu sprzętowego, takiego jak na przykład RSA SecurID f) potwierdzenia biometrycznego (odcisk palca, rozpoznawanie twarzy) 8. System umożliwia granularną (per aplikacja) kontrolę dostępu do aplikacji chmurowych lub znajdujących się w sieci lokalnej z wykorzystaniem drugiego (dodatkowego) składnika uwierzytelnienia.

	9. System umożliwia zbieranie oraz wyświetlanie logów dotyczących przebiegu procesu uwierzytelnienia zawierających następujące informacje: a) szczegółowy znacznik czasu (tzw. timestamp) opisujący minutę, godzinę, dzień, miesiąc i rok b) rezultat przebiegu procesu uwierzytelnienia (pozytywny, negatywny w zależności od tego czy dostęp został przyznany czy nie) c) nazwę użytkownika, który inicjował proces d) nazwę aplikacji, do której próbowano uzyskać dostęp e) urządzenie końcowe lub system operacyjny z którego nastąpiła próba uzyskania dostępu opatrzona dodatkowymi informacjami w postaci: f) przybliżonej lokalizacji urządzenia końcowego g) adresu IP urządzenia końcowego h) rodzaju użytego drugiego składnika uwierzytelnienia 10. System umożliwia wyświetlanie informacji dotyczących przebiegu procesu uwierzytelnienia na osi czasu (uwzględniając w/w rezultat przebiegu procesu uwierzytelnienia). 11. System umożliwia identyfikację urządzeń końcowych wykorzystywanych w procesie uwierzytelnienia dwuskładnikowego z rozróżnieniem na systemy operacyjne: a) macOS b) Windows c) Android d) iOS 12. System umożliwia identyfikację urządzeń końcowych wykorzystywanych w procesie uwierzytelnienia dwuskładnikowego z rozróżnieniem na: a) urządzenia mobilne b) laptopy oraz desktopy 13. Rozwiązanie objęte jest serwisem świadczonym bezpośrednio przez producenta uprawniającym do wsparcia technicznego w formie mailowej, telefonicznej lub czatu na czas trwania umowy. 14. System posiada publicznie dostępną dokumentację dla administratora oraz użytkownika. 15. System umożliwia administratorom rejestrację użytkowników w systemie chmurowym w następujące sposoby: a) Ręczne dodawanie pojedynczych użytkowników przez administratora b) Automatyczne dodawanie użytkowników dzięki synchronizacji z istniejącym Active Directory, Azure Active Directory lub OpenLDAP c) Zaimportowanie listy użytkowników z pliku CSV d) Samodzielną rejestracje użytkowników podczas logowania do niektórych aplikacji e) Samodzielną rejestrację użytkowników po uprzednim wysłaniu przez administratora maila lub wiadomości SMS z linkiem aktywacyjnym

	16. System oferuje możliwość samodzielnej rejestracji urządzenia wymaganego w procesie dwuskładnikowego uwierzytelniania przez użytkownika końcowego oraz możliwość zarządzania tymi urządzeniami. 17. System umożliwia konfigurację wielu metod uwierzytelniania oraz wybór wielu metod preferowanej i używanych jednocześnie przez użytkowników. 18. System umożliwia skonfigurowanie polityki obowiązującej nowych, jeszcze niezarejestrowanych użytkowników z możliwymi akcjami takimi jak: a) Wymaganie samodzielnej rejestracji przez użytkownika b) Zezwolenie na dostęp do aplikacji bez weryfikacji drugiego składnika uwierzytelniania c) Zablokowanie dostępu do aplikacji 19. System umożliwia administratorom włączenie opcji, która pozwala użytkownikom na zapamiętanie urządzenia końcowego przez ilość dni lub godzin zdefiniowanych przez administratora dla aplikacji webowych w celu uniknięcia ponownego procesu uwierzytelniania dwuskładnikowego przez określony czas. 20. System umożliwia konfiguracje zaufanych sieci w formacie adres IP, zakres adresów IP lub sieci CIDR w politykach, co umożliwia pominięcie dwuskładnikowego uwierzytelniania dla użytkowników znajdujących się wewnątrz zaufanej sieci. 21. System posiada REST API, umożliwiające programistyczny dostęp do funkcji administracyjnych oraz zarządzających. 22. System umożliwia administratorom zablokowanie używania wybranych metod uwierzytelniania przez użytkowników. 23. System nie posiada ograniczeń na ilość zabezpieczanych aplikacji. 24. System umożliwia tworzenie grup użytkowników i przypisywanie tych grup do aplikacji w celu pozwolenia na uwierzytelnienie do danej aplikacji tylko użytkownikom będącym częścią danej grupy. 25. System umożliwia administratorom wygenerowanie tymczasowego kodu dla użytkownika w celu pominięcia dwuskładnikowego uwierzytelniania. 26. System umożliwia personalizacje logo, które będzie wyświetlane użytkownikom w procesie uwierzytelniania dwuskładnikowego. 27. System umożliwia konfigurację limitu nieudanych prób uwierzytelnienia oraz ewentualne zablokowanie dostępu dla danego użytkownika. 28. System umożliwia integrację, w celu przeprowadzenia dwuskładnikowego uwierzytelnianie, z aplikacjami i systemami takimi jak: a) SSL lub IPSec VPN dla rozwiązań: Cisco Anyconnect opartych o Cisco ASA jak i Cisco FTD, Meraki Radius VPN, Checkpoint SSL VPN, Palo Alto Networks SSL VPN, Fortinet Fortigate SSL VPN, F5 SSL VPN, Juniper SSL VPN, SonicWall SRA SSL VPN, Array SSL VPN, Barracuda SSL VPN, OpenVPN. b) Rozwiązania dostępu zdalnego wspierające uwierzytelnianie poprzez RADIUS c) Serwisy Microsoft m.in. RDP, OWA

	d) Urządzenia i systemy wspierające uwierzytelnianie poprzez LDAP e) Własne aplikacje poprzez wbudowanie gotowej biblioteki WebSDK [dostępne języki programowania to m.in.: Python, Ruby, Java, PHP, Perl, Node.js] lub wykorzystanie REST API przeznaczonego do uwierzytelniania f) Aplikacje chmurowe przy użyciu SAML 2.0 [SSO]
Konsola zarządzająca	29. Wraz z rozwiązaniem dostarczona zostanie dedykowana konsola zarządzająca dostępna w chmurze. 30. Konsola zarządzająca jest dostępna przez interfejs WEB. 31. Konsola zarządzająca umożliwia monitorowanie aktywności w zakresie uwierzytelniania użytkowników w czasie rzeczywistym oraz centralne zarządzanie. 32. Konsola zarządzająca umożliwia zarządzanie, zgodnie z posiadaną licencją, następującymi elementami: a) Aplikacje b) Polityki c) Użytkownicy, w zakresie m.in.: ręczne dodawanie użytkowników pojedynczo, dodawanie listy użytkowników z pliku o formacie CSV, synchronizacja z Active Directory, zarządzanie samodzielną rejestracją użytkowników. d) Grupy użytkowników e) Urządzenia używane jako drugi składnik f) Wszystkie urządzenia końcowe g) Zaufane [firmowe] urządzenia końcowe – [licencja poziom III] h) Ustawienia dla administratorów 33. Konsola zarządzająca umożliwia dostęp do szczegółowych raportów zgodnie z posiadaną licencją w tym m.in.: a) Raport zawierający szczegółowe informacje odnośnie przebiegu procesu uwierzytelniania wraz z możliwością wyeksportowania raportu w formacie np. JSON lub `CSV b) Raport zawierający informacje dotyczące połączeń telefonicznych oraz wiadomości SMS użytych w procesie uwierzytelniania dwuskładnikowego wraz ze znacznikiem czasu oraz dokładnym numerem telefonu użytkownika z możliwością wyeksportowania raportu w formacie np. JSON, PDF lub CSV c) Raport zawierający informacje na temat akcji oraz zmian przeprowadzonych przez administratorów wraz ze znacznikiem czasu z możliwością wyeksportowania raportu w formacie np. JSON lub CSV d) Sumaryczny raport zawierający informacje na temat procesu uwierzytelniania wraz z przedstawieniem Top Aplikacji oraz Top Metod uwierzytelniania e) Raport przedstawiający informacje odnośnie nieudanych prób uwierzytelniania wraz z powodem niepowodzenia, a także m.in. Top odrzuconych użytkowników oraz aplikacji 34. Konsola zarządzająca umożliwia monitorowanie oraz elastyczne zarządzanie licencjami oraz płatnościami. 35. System umożliwia zdefiniowanie wielu administratorów o różnym poziomie uprawnień (RBAC).

	36. System umożliwia logowanie do portalu zarządzającego administratorom w oparciu o SSO. 37. System umożliwia podział użytkowników w logiczne domeny oraz do nich przypisanie konkretnych administratorów.
Zgodność z międzynarodowymi regulacjami	15. System spełnia wymagania uwierzytelniania wieloskładnikowego opisane w PCI-DSS 3.2 sekcja 8.3 16. System spełnia wymagania NIST 800-63 oraz 800-171 17. System jest zgodny z Ogólnym Rozporządzeniem o Ochronie Danych Osobowych RODO (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.) 18. System spełnia wymagania FFIEC dla aplikacji finansowych 19. System jest zgodny ze standardem SOC 2
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 1 sztuki Licencja na 1 rok dla 140 użytkowników

Część 6 : Akcesoria sieciowe

6.1 – Wkładki światłowodowe SFP28

Parametr	Wymagania
Rodzaj wkładki	SFP28
Przepustowość	25 Gb/s
Długość fali:	Tx 850 nm Rx: 850 nm
Minimalny zasięg transmisji	1m
Maksymalny zasięg transmisji	100m
Typ Złącza:	LC (Duplex)
Kompatybilne włókna optyczne	Multimode
Kombatybilność z urządzeniami producenta	Cisco
Gwarancja	1 rok
Stan	Fabrycznie nowy
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 4 sztuk

6.2 – Wkładki światłowodowe QSFP28

Parametr	Wymagania
Rodzaj wkładki	QSFP28
Przepustowość	100 Gb/s
Długość fali:	Tx 850 nm Rx: 850 nm
Minimalny zasięg transmisji	1m
Maksymalny zasięg transmisji	100m
Typ Złącza:	MPO
Kompatybilne włókna optyczne	Multimode
Kompatybilność z urządzeniami producenta	Cisco
Gwarancja	1 rok
Stan	Fabrycznie nowy
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 2 sztuk

6.3 – DEMUX 16 kanałowy CWDM

Parametr	Wymagania
Ilość kanałów	16
Obsługiwane fale	1271,1291,1311, 1331,1351,1371 ,1431,1451, 1471,1491,1511,1531,1551,1571,1591,1611 nm
Typ złącza	LC / APC
Gwarancja	1 rok
Stan	Fabrycznie nowy
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 1 sztuki

6.4 – Patchcord światłowodowy

Parametr	Wymagania
Typ złącza	MPO, typ B
Długość	3m
Typ złącza	LC / APC
Kompatybilne włókna optyczne	Multimode OM3
Gwarancja	1 rok
Stan	Fabrycznie nowy
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 1 sztuk

6.5 – Patchcord światłowodowy

Parametr	Wymagania
Typ złącza	LC, Duplex
Długość	3m
Typ złącza	LC / APC
Kompatybilne włókna optyczne	Multimode OM3
Gwarancja	1 rok
Stan	Fabrycznie nowy
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 2 sztuk

6.6 – Karta sieciowa

Specyfikacja sprzętu		
Ogólne	Interfejs magistrali hosta	PCIe 3.0 x8
	Wysokość mocowania	Niskoprofilowe i o pełnej wysokości
	Rozmiar (wys. x szer. x gł.)	69 mm x 168 mm x 17.3 mm
	Temperatura pracy	0°C do 40°C (32°F do 104°F)
	Temperatura przechowywania	-20°C do 60°C (-5°F do 140°F)

	Wilgotność względna	5% do 95% RH
	Gwarancja	5 lat
	Uwagi	Obsługa konfiguracji PCIe do wyższej przepustowości w celu zmniejszenia szerokości łącza i w rezultacie oszczędzania energii.
		Okres gwarancyjny rozpoczyna się od daty zakupu podanej na paragonie zakupu. (Dowiedz się więcej)
Sieć	Zgodność ze specyfikacją IEEE	IEEE 802.3ad Link Aggregation

		IEEE 802.3ae — 10Gbps Ethernet
	Szybkość transferu danych	10 Gbps
	Obsługiwane funkcje	Odciążanie segmentacji TCP (TSO)
		Odciążanie wysyłania dużej ilości danych (LSO)
		Skalowanie po stronie odbierającej (RSS)
		Ogólne odciążanie odbioru (GRO)
		Ogólne odciążanie segmentacji (GSO)
		1,5-9 KB Jumbo Frame

		Przechowywanie z przenoszeniem przez sieć Ethernet
		Przechowywanie bez przenoszenia przez sieć Ethernet
		Przenoszenie sumy kontrolnej TCP/UDP
		Skalowanie po stronie nadającej (TSS)
		SR-IOV
Zgodność	Zgodność ze sprzętem Synology DS1621xs+ lub kompatybilne.	
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 1 sztuki	

Cześć 7 : Oprogramowanie typu EDR

Parametr	Wymagania
Typ	Oprogramowanie typu EDR Endpoint Detection and Response
Wymagania ogólne	W ramach dostawy Zamawiający wymaga dostarczenia licencji oprogramowania antywirusowego z funkcjonalnością EDR na okres 24 miesięcy, dla 110 stanowisk.
OPIS– wymagania minimalne:	
Administracja zdalna w chmurze	1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11) posiadane przez Zamawiającego. 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi integrować się z Intel Threat Detection Technology. 11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

	• tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. 23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: • tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, • tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. 24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. 25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez

	odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. 29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
Ochrona serwera	1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. Dodatkowe wymagania dla ochrony serwerów Windows: 9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej. 10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V posiadanego przez Zamawiającego. 12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci

	masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe wymagania dla ochrony serwerów Linux: 18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 20. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
Szyfrowanie	1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem. 3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
Ochrona urządzeń mobilnych opartych o system Android	1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.

	5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: a. usunięcie zawartości urządzenia, b. przywrócenie urządzenie do ustawień fabrycznych, c. zablokowania urządzenia, d. uruchomienie sygnału dźwiękowego, e. lokalizację GPS. 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła.
Sandbox w chmurze	1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 2. Rozwiązanie musi wykorzystywać do działania chmurę producenta. 3. Rozwiązanie musi posiadać możliwość 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. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. 6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. 8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. 9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. 11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. 12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: a) Czysty, b) Podejrzany, c) Bardzo podejrzany,

	d) Szkodliwy. 13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. 14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. 15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia
Moduł XDR	1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. 6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. 7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. 9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. 13. W ramach przeglądania wykonanego skryptu, administrator musi

	posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. 14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. 15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich. 16. Konsola administracyjna musi mieć możliwość tagowania obiektów. 17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
Wymagania dodatkowe	Zamawiający wymaga aby Wykonawca dokonał wdrożenia proponowanego rozwiązania. W ramach wdrożenia rozwiązania zamawiający wymaga w zakresie minimum: - Instalacja serwera konsoli EDR na maszynie wskazanej przez Zamawiającego; - Wstępna konfuguracja; - Przygotowanie wstepnych, domyślnych polityk; - Wdrożenie agenta EDR - Sprawdzenie poprawności działania serwera konsoli EDR - Przegląd detekcji zgromadzonych w konsoli - Wspólna analiza i optymalizacja, - Wspólne tworzenie wykluczeń Wymagane jest aby wdrożenie przeprowadzone było przez Inżyniera Wykonawcy, posiadającego certyfikat producenta dostarczanego rozwiązania.
Ilość	1 szt.

Część 8 : Pamięć masowa

8.1 – Dyski twarde 3,5 cala

Specyfikacja sprzętu		
Ogólne	Pojemność minimalna.	16 TB
	Obudowa	3.5"
	Interfejs	SATA 6 Gb/s
	Rozmiar sektora	512e
Wydajność	Prędkość obrotowa	7,200 rpm
	Szybkość interfejsu	6.0 Gb/s, 3.0 Gb/s, 1.5 Gb/s
	Rozmiar buforu	512 MiB
	Maksymalna stała prędkość przesyłu danych (typ.)	262 MiB/s
Niezawodność	Średni czas do awarii (MTTF)	2.5 mln godzin
	Ocena obciążenia	550 TB przeniesionych danych rocznie
	Gwarancja	5 lat
	Uwagi	
Zużycie energii	Napięcie zasilania	12 V (± 10%) / 5 V (+10/-7%)
	Aktywny tryb bezczynności (typ.)	4.00 W
	Losowy odczyt/zapis (4 KB Q1) (typ.)	7.63 W
	Uwagi	
Temperatura	Działa	5°C do 60°C (41°F do 140°F)
	Nie działa	-40°C do 70°C (-40°F do 158°F)
Wstrząs	Działa	686 m/s^2 {70 G} (czas trwania 2 ms)
	Nie działa	2450 m/s^2 {250 G} (czas trwania 2 ms)
Drgania	Działa	7,35 m/s^2 {0.75 G} (od 5 do 300 Hz), 2,45 m/s^2 {0.25 G} (od 300 do 500 Hz)
	Nie działa	29,4 m/s^2 {3.0 G} (od 5 do 500 Hz)
Wysokość	Działa	-305 metry do 3,048 metry
	Nie działa	-305 metry do 12,192 metry
Wilgotność względna	Działa	5-90% R.H. (bez kondensacji)
	Nie działa	5-95% R.H. (bez kondensacji)
Inne	Rozmiar (wys. x szer. x gł.)	26.1 mm x 101.85 mm x 147 mm

	Masa	720 g
	Certyfikaty	CE
		EAC
		BSMI
		RCM
		KC
		RoHS
		ICES
		TUV
		UL
	Zgodność.	Zgodność i wsparcie sprzętowe Synology DS1621xs+ lub równoważne .
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 4 sztuk	

Część 8.2 : Dyski SSD m2

Ogólne	Pojemność	800 GB
	Obudowa	M.2 2280
	Interfejs	NVMe PCIe 3.0 x4
Wydajność	Stały odczyt sekwencyjny (128 KB, QD32)	3,100 MB/s
	Stały zapis sekwencyjny (128 KB, QD32)	1,000 MB/s
	Stały odczyt losowy (4KB, QD256)	400,000 IOPS
	Stały zapis losowy (4KB, QD256)	70,000 IOPS

	Uwagi	Wszystkie pomiary wydajności zostały uzyskane w pełnym zrównoważonym trybie w oparciu o obciążenie biznesowe JESD219A określone przez stowarzyszenie JEDEC Solid State Technology Association.
Wytrzymałość i niezawodność	Zapisane terabajty (TBW)*	1,022 TB
	Średni czas do awarii (MTBF)	1.8 mln godzin
	UBER (bitowa stopa nienaprawialnych błędów)	< 1 sector per 10^{17} bits read
	Zabezpieczenie przed utratą zasilania	-
	Gwarancja*	5 lat

		W oparciu o obciążenie biznesowe JESD219A.
	Uwagi	Okres gwarancyjny rozpoczyna się od daty zakupu podanej na paragonie zakupu. (Dowiedz się więcej)
Zużycie energii	Napięcie zasilania	3.3V (± 5%)
	Aktywny odczyt (typ.)	5.5 W
	Aktywny zapis (typ.)	4.6 W
	Bezczynny	1.6 W
	Uwagi	Zużycie energii może się różnić w zależności od konfiguracji i platform.
Temperatura	Temperatura pracy	0°C do 70°C (32°F do 158°F)

	Temperatura przechowywania	-40°C do 85°C (-40°F do 185°F)
Inne	Rozmiar (wys. x szer. x gł.)	3.5 mm x 22 mm x 80 mm
	Certyfikaty	FCC
		CE
		EAC
		BSMI
		VCCI
		RCM
		KC
		RoHS
		UKCA
	Zgodność.	Zgodność ze sprzętem Synology DS1621xs+ lub rówoważne.
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 2 sztuk	

Część 9 : Licencje MacSec

Parametr	**Wymagania**
Typ licencji	Licencja pozwalająca uruchomić IEEE 802.1ae MACsec na przełącznikach posiadanych przez Zamawiającego – Juniper EX3400-48P
Ważność licencji	Wieczysta
Ilość licencji	Liczba licencji musi pozwalać na uruchomienie protokołu IEEE 802.1ae MACsec na 8 ww. przełącznikach sieciowych
Stan	Fabrycznie nowy