

Załącznik numer 4 do SWZ

Cześć 1 : Zapora antyspamowa

Parametr	Wymagania	
Wymagania ogólne	<p>System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.</p> <p>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 systemu 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.</p> <p>Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.</p> <p>Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:</p> <ol style="list-style-type: none"> 1. Tryb Gateway. 2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej). 	Spełnia / nie spełnia
Parametry fizyczne systemu antyspamowego	System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.	Spełnia / nie spełnia
Ogólne funkcje systemu ochrony poczty	Wsparcie dla co najmniej 20 domen pocztowych	Spełnia / nie spełnia
	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).	Spełnia / nie spełnia

	Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.	Spełnia / nie spełnia
	Zarządzanie kolejkami wiadomości (np. reguły opóźnienia dostarczenia wiadomości).	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia
	Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.	Spełnia / nie spełnia
	Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.	Spełnia / nie spełnia
	Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.	Spełnia / nie spełnia
	Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.	Spełnia / nie spełnia
	Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.	Spełnia / nie spełnia
	Dostęp do kwarantanny użytkownika możliwy poprzez WebMail. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia
	3. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.	Spełnia / nie spełnia
	4. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.	Spełnia / nie spełnia

	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.	Spełnia / nie spełnia
Kontrola antywirusowa i ochrona przed malware	Skanowanie antywirusowe wiadomości SMTP	Spełnia / nie spełnia
	Kwarantannę dla zainfekowanych plików.	Spełnia / nie spełnia
	Skanowanie załączników skompresowanych.	Spełnia / nie spełnia
	Definiowanie komunikatów powiadomień w języku polskim.	Spełnia / nie spełnia
	Blokowanie załączników w oparciu o typ pliku.	Spełnia / nie spełnia
	Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.	Spełnia / nie spełnia
	Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętowa lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanymi dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia
Ochronę typu wirus outbrake.	Spełnia / nie spełnia	
Kontrola antyspamowa	Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.	Spełnia / nie spełnia
	Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.	Spełnia / nie spełnia
	Szczegółowa kontrola nagłówka wiadomości.	Spełnia / nie spełnia
	Analiza Heurystyczna.	Spełnia / nie spełnia
	Współpraca z zewnętrznymi serwerami RBL, SURBL.	Spełnia / nie spełnia

	Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.	Spełnia / nie spełnia
	Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.	Spełnia / nie spełnia
	Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.	Spełnia / nie spełnia
	Kontrola w oparciu o Greylisting oraz SPF.	Spełnia / nie spełnia
	Filtrowanie treści wiadomości i załączników.	Spełnia / nie spełnia
	Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.	Spełnia / nie spełnia
	Ochrona typu outbrake. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia
Ochrona przed atakami na usługę poczty	Ochrona przed atakami na adres odbiorcy (m.in. email bombing)	Spełnia / nie spełnia
	Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.	Spełnia / nie spełnia
	Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.	Spełnia / nie spełnia
	Kontrola Reverse DNS (ochrona przed Anty-Spoofing).	Spełnia / nie spełnia
	Weryfikacja poprawności adresu e-mail nadawcy.	Spełnia / nie spełnia
Funkcje logowania i raportowania	Logowanie do zewnętrznego serwera SYSLOG.	Spełnia / nie spełnia
	Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.	Spełnia / nie spełnia
	Logowanie informacji na temat spamu oraz niedozwolonych załączników.	Spełnia / nie spełnia
	Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.	Spełnia / nie spełnia

	Możliwość analizy przebiegu sesji SMTP.	Spełnia / nie spełnia
	Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.	Spełnia / nie spełnia
	Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.	Spełnia / nie spełnia
	Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.	Spełnia / nie spełnia
Funkcje pracy w trybie wysokiej dostępności (HA)	Konfigurację HA w każdym z trybów: gateway, transparent.	Spełnia / nie spełnia
	Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.	Spełnia / nie spełnia
	Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.	Spełnia / nie spełnia
	Monitorowanie stanu pracy klastra.	Spełnia / nie spełnia
Aktualizacje sygnatur, dostęp do bazy spamu	Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.	Spełnia / nie spełnia
	Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.	Spełnia / nie spełnia
Zarządzanie	System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.	Spełnia / nie spełnia
	Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.	Spełnia / nie spełnia
	Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.	Spełnia / nie spełnia

Certyfikaty	Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji : VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.	Spełnia / nie spełnia
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.	Spełnia / nie spełnia
Gwarancja oraz wsparcie	System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.	Spełnia / nie spełnia
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.	Spełnia / nie spełnia
	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	Spełnia / nie spełnia
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 1 sztuki	Spełnia / nie spełnia

Cześć 2 : Serwer NAS

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

Zasilanie	Zasilacz redundatny 2 x 550 W, 100-240 V	Spełnia / nie spełnia
		Spełnia / nie spełnia
		Spełnia / nie spełnia
Specyfikacja oprogramowania		
Agregacja łączy	Tak	Spełnia / nie spełnia
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+	Spełnia / nie spełnia
Możliwość podłączenia karty WLAN na USB	Tak	Spełnia / nie spełnia
Szyfrowanie wolumenów	Tak, min AES 256	Spełnia / nie spełnia
Szyfrowanie dysków zewnętrznych	Tak	Spełnia / nie spełnia
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	Spełnia / nie spełnia
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	Spełnia / nie spełnia
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	Spełnia / nie spełnia
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP	Spełnia / nie spełnia
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,	Spełnia / nie spełnia

Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business, Box	Spełnia / nie spełnia
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android	Spełnia / nie spełnia
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediiów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu	Spełnia / nie spełnia
VPN	VPN client / VPN server Obsługa PPTP, OpenVPN	Spełnia / nie spełnia
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	Spełnia / nie spełnia
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.	Spełnia / nie spełnia
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXI i Docker	Spełnia / nie spełnia

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	Spełnia / nie spełnia
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek	Spełnia / nie spełnia
		Spełnia / nie spełnia
Gwarancja	3 lata	Spełnia / nie spełnia
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 1 sztuki	Spełnia / nie spełnia

Cześć 3 : Oprogramowanie do backupu

	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,	Spełnia / nie spełnia
Wymagania ogólne	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	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia
Całkowite koszty posiadania	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej	Spełnia / nie spełnia

Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków	Spełnia / nie spełnia
Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków	Spełnia / nie spełnia
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	Spełnia / nie spełnia
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.	Spełnia / nie spełnia
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.	Spełnia / nie spełnia
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.	Spełnia / nie spełnia
Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.	Spełnia / nie spełnia
Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania	Spełnia / nie spełnia
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)	Spełnia / nie spełnia
Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu	Spełnia / nie spełnia

	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	Spełnia / nie spełnia
	Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiegokolwiek funkcjonalności wymienionej w tej specyfikacji	Spełnia / nie spełnia
	Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania	Spełnia / nie spełnia
	Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.	Spełnia / nie spełnia
	Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej	Spełnia / nie spełnia
	Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora)	Spełnia / nie spełnia
	Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS)	Spełnia / nie spełnia
	Oprogramowanie musi posiadać integracje z systemami typu SIEM	Spełnia / nie spełnia
	Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.	Spełnia / nie spełnia
Wymagania RPO	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej	Spełnia / nie spełnia
	Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.	Spełnia / nie spełnia
	Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być	Spełnia / nie spełnia

	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.	Spełnia / nie spełnia
	Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.	Spełnia / nie spełnia
	Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).	Spełnia / nie spełnia
	Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)	Spełnia / nie spełnia
	Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia
	Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia
	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 punktu w ramach ustalonego parametru RPO.	Spełnia / nie spełnia
	Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik	Spełnia / nie spełnia

	Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)	Spełnia / nie spełnia
	Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)	Spełnia / nie spełnia
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.	Spełnia / nie spełnia
	Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)	Spełnia / nie spełnia
	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	Spełnia / nie spełnia
	Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia
	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków	Spełnia / nie spełnia
	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.	Spełnia / nie spełnia
	Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta	Spełnia / nie spełnia

	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.	Spełnia / nie spełnia
	Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell	Spełnia / nie spełnia
	Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM	Spełnia / nie spełnia
	Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia

	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.	Spełnia / nie spełnia
	Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.	Spełnia / nie spełnia
	Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji	Spełnia / nie spełnia
	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN	Spełnia / nie spełnia
	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle	Spełnia / nie spełnia
	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI	Spełnia / nie spełnia
	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2	Spełnia / nie spełnia
	Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN	Spełnia / nie spełnia
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 uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)	Spełnia / nie spełnia
	Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.	Spełnia / nie spełnia
	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	Spełnia / nie spełnia
	Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem	Spełnia / nie spełnia

	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	Spełnia / nie spełnia
	Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania	Spełnia / nie spełnia
	Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków	Spełnia / nie spełnia
	Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.	Spełnia / nie spełnia
	Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR	Spełnia / nie spełnia
Środowiska fizyczne	Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego	Spełnia / nie spełnia
	Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych	Spełnia / nie spełnia
	Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, Rocky Linux, AlmaLinux	Spełnia / nie spełnia
	Rozwiązanie musi wspierać system operacyjny macOS	Spełnia / nie spełnia
	Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix	Spełnia / nie spełnia
	Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)	Spełnia / nie spełnia
	Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster	Spełnia / nie spełnia
	Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk	Spełnia / nie spełnia

	całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów	
	Rozwiązanie musi wspierać backup podłączonych dysków USB	Spełnia / nie spełnia
	Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym	Spełnia / nie spełnia
	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)	Spełnia / nie spełnia
	Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone	Spełnia / nie spełnia
	Rozwiązanie musi wspierać kontrolę pasma sieciowego	Spełnia / nie spełnia
	Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych	Spełnia / nie spełnia
	Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN	Spełnia / nie spełnia
	Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft	Spełnia / nie spełnia
	Rozwiązanie musi wspierać technologię BitLocker	Spełnia / nie spełnia
	Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania	Spełnia / nie spełnia
	Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednorazowej 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	Spełnia / nie spełnia
	Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych	Spełnia / nie spełnia

	Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle i PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.	Spełnia / nie spełnia
	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	Spełnia / nie spełnia
	Rozwiązanie musi wspierać szyfrowanie	Spełnia / nie spełnia
	Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne	Spełnia / nie spełnia
	Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczonego Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej	Spełnia / nie spełnia
	Rozwiązanie musi wspierać tworzenie wielu zadań backupowych	Spełnia / nie spełnia
Monitoring	System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich	Spełnia / nie spełnia
	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	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia
	System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter	Spełnia / nie spełnia
	System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn	Spełnia / nie spełnia

	System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel	Spełnia / nie spełnia
	System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk	Spełnia / nie spełnia
	System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora	Spełnia / nie spełnia
	System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów	Spełnia / nie spełnia
	System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)	Spełnia / nie spełnia
	System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna	Spełnia / nie spełnia
	System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego	Spełnia / nie spełnia
	System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta	Spełnia / nie spełnia
	System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.	Spełnia / nie spełnia
	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.	Spełnia / nie spełnia
	System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware	Spełnia / nie spełnia
	System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.6	Spełnia / nie spełnia
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	Spełnia / nie spełnia

	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.	Spełnia / nie spełnia
	System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.	Spełnia / nie spełnia
	System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V	Spełnia / nie spełnia
	System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF	Spełnia / nie spełnia
	System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc	Spełnia / nie spełnia
	System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach	Spełnia / nie spełnia
	System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów	Spełnia / nie spełnia
	System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych	Spełnia / nie spełnia
	System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych	Spełnia / nie spełnia
	System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury	Spełnia / nie spełnia
	System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta	Spełnia / nie spełnia
	System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań	Spełnia / nie spełnia

	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'.	Spełnia / nie spełnia
	System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware	Spełnia / nie spełnia
	System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)	Spełnia / nie spełnia
	System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie	Spełnia / nie spełnia

Cześć 4 : Przełącznik sieciowy

Parametr	Wymagania	
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn, wyposażona w zintegrowany zasilacz HotPlug, możliwość instalacji drugiego redundantnego zasilacza.	Spełnia / nie spełnia
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.	Spełnia / nie spełnia
Wydajność przełącznika	<ul style="list-style-type: none"> - 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 	Spełnia / nie spełnia

Funkcjonalność warstwy II	<ul style="list-style-type: none"> - 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 	Spełnia / nie spełnia
Funkcjonalność warstwy III	<ul style="list-style-type: none"> - obsługa minimum 3000 wpisów routingu IPv4 - obsługa minimum 1500 wpisów routingu IPv4 - obsługa routingu statycznego oraz RIPv2 - obsługa PBR 	Spełnia / nie spełnia
Zgodność z protokołami / standardami	<p>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</p>	Spełnia / nie spełnia
Zarządzanie siecią i bezpieczeństwo	<p>Sprzęt musi obsługiwać zarządzanie poprzez narzędzie do centralnego monitorowania i zarządzania oferowane przez producenta urządzenia. Zarządzanie z CLI</p>	Spełnia / nie spełnia
Warunki pracy	<ul style="list-style-type: none"> - temperatura pracy w zakresie od 0 do 40 stopni Celsjusza - wilgotność dla trybu pracy 10% do 85% bez kondensacji 	Spełnia / nie spełnia

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	Spełnia / nie spełnia
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.	Spełnia / nie spełnia
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.	Spełnia / nie spełnia
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 2 sztuk	Spełnia / nie spełnia

Cześć 5 : Autentykator MFA

Parametr	Wymagania	
Architektura	<ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> a) pierwszy składnik uwierzytelnienia przetrzymywany jest w ramach wyodrębnionego systemu trzeciego IdP tzw. (Identity Provider) 	Spełnia / nie spełnia

	<ul style="list-style-type: none"> 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 <p>5. Komponent IdP umożliwia zarówno instalację lokalną (on premise) jak i w środowisku chmurowym.</p> <p>6. System chmurowy odpowiedzialny za drugi składnik uwierzytelniania zbudowany jest w oparciu o odporną na awarię architekturę wysokiej klasy oraz charakteryzuje się wysoką dostępnością infrastruktury.</p>	
<p>Funkcjonalność systemu</p>	<p>7. System umożliwia kontrolę dostępu do aplikacji chmurowych lub znajdujących się w sieci lokalnej z wykorzystaniem drugiego (dodatkowego) składnika uwierzytelnienia w postaci:</p> <ul style="list-style-type: none"> 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) <p>8. System umożliwia granularną (per aplikacja) kontrolę dostępu do aplikacji chmurowych lub znajdujących się w sieci lokalnej z wykorzystaniem drugiego (dodatkowego) składnika uwierzytelnienia.</p> <p>9. System umożliwia zbieranie oraz wyświetlanie logów dotyczących przebiegu procesu uwierzytelnienia zawierających następujące informacje:</p> <ul style="list-style-type: none"> 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 	<p>Spełnia / nie spełnia</p>

	<p>opatrzona dodatkowymi informacjami w postaci:</p> <ul style="list-style-type: none"> f) przybliżonej lokalizacji urządzenia końcowego g) adresu IP urządzenia końcowego h) rodzaju użytego drugiego składnika uwierzytelnienia <p>10. System umożliwia wyświetlanie informacji dotyczących przebiegu procesu uwierzytelnienia na osi czasu (uwzględniając w/w rezultat przebiegu procesu uwierzytelnienia).</p> <p>11. System umożliwia identyfikację urządzeń końcowych wykorzystywanych w procesie uwierzytelnienia dwuskładnikowego z rozróżnieniem na systemy operacyjne:</p> <ul style="list-style-type: none"> a) macOS b) Windows c) Android d) iOS <p>12. System umożliwia identyfikację urządzeń końcowych wykorzystywanych w procesie uwierzytelnienia dwuskładnikowego z rozróżnieniem na:</p> <ul style="list-style-type: none"> a) urządzenia mobilne b) laptopy oraz desktopy <p>13. Rozwiązanie objęte jest serwisem świadczonym bezpośrednio przez producenta</p> <p>uprawniającym do wsparcia technicznego w formie mailowej , telefonicznej lub czatu na czas trwania umowy.</p> <p>14. System posiada publicznie dostępną dokumentację dla administratora oraz użytkownika.</p> <p>15. System umożliwia administratorom rejestrację użytkowników w systemie chmurowym w następujące sposoby:</p> <ul style="list-style-type: none"> 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 rejestrację użytkowników podczas logowania do niektórych aplikacji e) Samodzielną rejestrację użytkowników po uprzednim wysłaniu przez administratora maila lub wiadomości SMS z linkiem aktywacyjnym <p>16. System oferuje możliwość samodzielnej rejestracji urządzenia wymaganego w procesie dwuskładnikowego uwierzytelniania przez użytkownika końcowego oraz możliwość zarządzania tymi urządzeniami.</p> <p>17. System umożliwia konfigurację wielu metod uwierzytelniania oraz</p>	
--	--	--

	<p>wybór wielu metod preferowanej i używanych jednocześnie przez użytkowników.</p> <p>18. System umożliwia skonfigurowanie polityki obowiązującej nowych, jeszcze niezarejestrowanych użytkowników z możliwymi akcjami takimi jak:</p> <ol style="list-style-type: none"> a) Wymaganie samodzielnej rejestracji przez użytkownika b) Zezwolenie na dostęp do aplikacji bez weryfikacji drugiego składnika uwierzytelniania c) Zablokowanie dostępu do aplikacji <p>19. System umożliwia administratorom włączenie opcji, która pozwala użytkownikom na zapamiętanie urzędzenia końcowego przez ilość dni lub godzin zdefiniowanych przez administratora dla aplikacji webowych w celu uniknięcia ponownego procesu uwierzytelniania dwuskładnikowego przez określony czas.</p> <p>20. System umożliwia konfigurację 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.</p> <p>21. System posiada REST API, umożliwiające programistyczny dostęp do funkcji administracyjnych oraz zarządzających.</p> <p>22. System umożliwia administratorom zablokowanie używania wybranych metod uwierzytelniania przez użytkowników.</p> <p>23. System nie posiada ograniczeń na ilość zabezpieczanych aplikacji.</p> <p>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.</p> <p>25. System umożliwia administratorom wygenerowanie tymczasowego kodu dla użytkownika w celu pominięcia dwuskładnikowego uwierzytelniania.</p> <p>26. System umożliwia personalizację logo, które będzie wyświetlane użytkownikom w procesie uwierzytelniania dwuskładnikowego.</p> <p>27. System umożliwia konfigurację limitu nieudanych prób uwierzytelnienia oraz ewentualne zablokowanie dostępu dla danego użytkownika.</p> <p>28. System umożliwia integrację, w celu przeprowadzenia dwuskładnikowego uwierzytelniania, z aplikacjami i systemami takimi jak:</p> <ol style="list-style-type: none"> a) SSL lub IPSec VPN dla rozwiązań: Cisco Anyconnect o partych o Cisco ASA jak i Cisco 	
--	---	--

	<p>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.</p> <p>b) Rozwiązania dostępu zdalnego wspierające uwierzytelnianie poprzez RADIUS</p> <p>c) Serwisy Microsoft m.in. RDP, OWA</p> <p>d) Urządzenia i systemy wspierające uwierzytelnianie poprzez LDAP</p> <p>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</p> <p>f) Aplikacje chmurowe przy użyciu SAML 2.0 [SSO]</p>	
Konsola zarządzająca	<p>29. Wraz z rozwiązaniem dostarczona zostanie dedykowana konsola zarządzająca dostępna w chmurze.</p> <p>30. Konsola zarządzająca jest dostępna przez interfejs WEB.</p> <p>31. Konsola zarządzająca umożliwia monitorowanie aktywności w zakresie uwierzytelniania użytkowników w czasie rzeczywistym oraz centralne zarządzanie.</p> <p>32. Konsola zarządzająca umożliwia zarządzanie, zgodnie z posiadaną licencją, następującymi elementami:</p> <p>a) Aplikacje</p> <p>b) Polityki</p> <p>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.</p> <p>d) Grupy użytkowników</p> <p>e) Urządzenia używane jako drugi składnik</p> <p>f) Wszystkie urządzenia końcowe</p> <p>g) Zaufane [firmowe] urządzenia końcowe – [licencja poziom III]</p> <p>h) Ustawienia dla administratorów</p> <p>33. Konsola zarządzająca umożliwia dostęp do szczegółowych raportów zgodnie z posiadaną licencją w tym m.in.:</p> <p>a) Raport zawierający szczegółowe informacje odnośnie przebiegu procesu uwierzytelniania wraz z możliwością wyeksportowania raportu w formacie np. JSON lub `CSV</p>	Spełnia / nie spełnia

	<p>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</p> <p>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</p> <p>d) Sumaryczny raport zawierający informacje na temat procesu uwierzytelniania wraz z przedstawieniem Top Aplikacji oraz Top Metod uwierzytelniania</p> <p>e) Raport przedstawiający informacje odnośnie nieudanych prób uwierzytelniania wraz z powodem niepowodzenia, a także m.in. Top odrzuconych użytkowników oraz aplikacji</p> <p>34. Konsola zarządzająca umożliwia monitorowanie oraz elastyczne zarządzanie licencjami oraz płatnościami.</p> <p>35. System umożliwia zdefiniowanie wielu administratorów o różnym poziomie uprawnień (RBAC).</p> <p>36. System umożliwia logowanie do portalu zarządzającego administratorom w oparciu o SSO.</p> <p>37. System umożliwia podział użytkowników w logiczne domeny oraz do nich przypisanie konkretnych administratorów.</p>	
Zgodność z międzynarodowymi regulacjami	<p>15. System spełnia wymagania uwierzytelniania wieloskładnikowego opisane w PCI-DSS 3.2 sekcja 8.3</p> <p>16. System spełnia wymagania NIST 800-63 oraz 800-171</p> <p>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.)</p> <p>18. System spełnia wymagania FFIEC dla aplikacji finansowych</p> <p>19. System jest zgodny ze standardem SOC 2</p>	Spełnia / nie spełnia
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 1 sztuki Licencja na 1 rok dla 140 użytkowników	Spełnia / nie spełnia

Część 6 : Akcesoria sieciowe

6.1 – Wkładki światłowodowe SFP28

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

6.2 – Wkładki światłowodowe QSFP28

Parametr	Wymagania	
Rodzaj wkładki	QSFP28	Spełnia / nie spełnia
Przepustowość	100 Gb/s	Spełnia / nie spełnia
Długość fali:	Tx 850 nm Rx: 850 nm	Spełnia / nie spełnia
Minimalny zasięg transmisji	1m	Spełnia / nie spełnia
Maksymalny zasięg transmisji	100m	Spełnia / nie spełnia
Typ Złącza:	MPO	Spełnia / nie spełnia

Kompatybilne włókna optyczne	Multimode	Spełnia / nie spełnia
Kompatybilność z urządzeniami producenta	Cisco	Spełnia / nie spełnia
Gwarancja	1 rok	Spełnia / nie spełnia
Stan	Fabrycznie nowy	Spełnia / nie spełnia
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 2 sztuk	

6.3 – DEMUX 16 kanałowy CWDM

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

6.4 – Patchcord światłowodowy

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

6.5 – Patchcord światłowodowy

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

6.6 – Karta sieciowa

Specyfikacja sprzętu			
Ogólne			Spełnia / nie spełnia
	Interfejs magistrali hosta	PCIe 3.0 x8	Spełnia / nie spełnia
	Wysokość mocowania	Niskoprofilowe i o pełnej wysokości	Spełnia / nie spełnia
	Rozmiar (wys. x szer. x gł.)	69 mm x 168 mm x 17.3 mm	Spełnia / nie spełnia
	Temperatura pracy	0°C do 40°C (32°F do 104°F)	Spełnia / nie spełnia
	Temperatura przechowywania	-20°C do 60°C (-5°F do 140°F)	Spełnia / nie spełnia
	Wilgotność względna	5% do 95% RH	Spełnia / nie spełnia
	Gwarancja	5 lat	Spełnia / nie spełnia

			Spełnia / nie spełnia
	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)	Spełnia / nie spełnia
			Spełnia / nie spełnia
Sieć	Zgodność ze specyfikacją IEEE	IEEE 802.3ad Link Aggregation	Spełnia / nie spełnia
		IEEE 802.3ae — 10Gbps Ethernet	Spełnia / nie spełnia
			Spełnia / nie spełnia
	Szybkość transferu danych	10 Gbps	Spełnia / nie spełnia

Obsługiwane funkcje	Odciążanie segmentacji TCP (TSO)	Spełnia / nie spełnia
	Odciążanie wysyłania dużej ilości danych (LSO)	Spełnia / nie spełnia
	Skalowanie po stronie odbierającej (RSS)	Spełnia / nie spełnia
	Ogólne odciążanie odbioru (GRO)	Spełnia / nie spełnia
	Ogólne odciążanie segmentacji (GSO)	Spełnia / nie spełnia
	1,5-9 KB Jumbo Frame	Spełnia / nie spełnia
	Przechowywanie z przenoszeniem przez sieć Ethernet	Spełnia / nie spełnia
	Przechowywanie bez przenoszenia przez sieć Ethernet	Spełnia / nie spełnia

		Przenoszenie sumy kontrolnej TCP/UDP	Spełnia / nie spełnia
		Skalowanie po stronie nadającej (TSS)	Spełnia / nie spełnia
		SR-IOV	Spełnia / nie spełnia
Zgodność	Zgodność ze sprzętem Synology DS1621xs+ lub kompatybilne.		Spełnia / nie spełnia
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 1 sztuki		Spełnia / nie spełnia

Cześć 7 : Oprogramowanie typu EDR

Parametr	Wymagania	
Typ	Oprogramowanie typu EDR Endpoint Detection and Response	Spełnia / nie spełnia
Wymagania ogólne	W ramach dostawy Zamawiający wymaga dostarczenia licencji oprogramowania antywirusowego z funkcjonalnością EDR na okres 24 miesięcy, dla 110 stanowisk.	Spełnia / nie spełnia
OPIS– wymagania minimalne:		
Administracja zdalna w chmurze	<ol style="list-style-type: none"> 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. 	Spełnia / nie spełnia

	<p>5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.</p> <p>6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.</p> <p>7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.</p> <p>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.</p> <p>9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.</p> <p>10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.</p> <p>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.</p> <p>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.</p>	
<p>Ochrona stacji roboczych</p>	<p>1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11) posiadane przez Zamawiającego.</p> <p>2. Rozwiązanie musi wspierać architekturę ARM64.</p> <p>3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.</p> <p>4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.</p> <p>5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.</p> <p>6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.</p>	<p>Spełnia / nie spełnia</p>

	<p>7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.</p> <p>8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.</p> <p>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.</p> <p>10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.</p> <p>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).</p> <p>12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:</p> <ul style="list-style-type: none">• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,	
--	---	--

	<ul style="list-style-type: none"> • 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. <p>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.</p> <p>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.</p> <p>19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p> <p>20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).</p> <p>21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.</p> <p>23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:</p> <ul style="list-style-type: none"> • 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, 	
--	---	--

	<ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> 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, 	Spełnia / nie spełnia

	<p>w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. Dodatkowe wymagania dla ochrony serwerów Windows:</p> <p>9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej.</p> <p>10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).</p> <p>11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V posiadanego przez Zamawiającego.</p> <p>12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>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.</p> <p>14. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.</p> <p>15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.</p> <p>16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.</p> <p>17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe wymagania dla ochrony serwerów Linux:</p> <p>18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.</p> <p>19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.</p> <p>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</p>	
--	---	--

	to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonoego mikro-serwisu.	
Szyfrowanie	<ol style="list-style-type: none"> 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 autentykację 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. 	Spełnia / nie spełnia
Ochrona urządzeń mobilnych opartych o system Android	<ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła. 	Spełnia / nie spełnia
Sandbox w chmurze	<ol style="list-style-type: none"> 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 	Spełnia / nie spełnia

	<p>archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.</p> <p>4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.</p> <p>5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.</p> <p>6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.</p> <p>7. Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów.</p> <p>8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.</p> <p>9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.</p> <p>10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.</p> <p>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.</p> <p>12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:</p> <ul style="list-style-type: none"> a) Czysty, b) Podejrzany, c) Bardzo podejrzany, d) Szkodliwy. <p>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.</p> <p>14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.</p> <p>15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia</p>	
Moduł XDR	<p>1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.</p> <p>2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.</p>	Spełnia / nie spełnia

	<p>3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.</p> <p>4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.</p> <p>5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.</p> <p>6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.</p> <p>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.</p> <p>13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.</p> <p>14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji</p>	
--	--	--

	<p>powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.</p> <p>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.</p> <p>16. Konsola administracyjna musi mieć możliwość tagowania obiektów.</p> <p>17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.</p>	
Wymagania dodatkowe	<p>Zamawiający wymaga aby Wykonawca dokonał wdrożenia proponowanego rozwiązania. W ramach wdrożenia rozwiązania zamawiający wymaga w zakresie minimum:</p> <ul style="list-style-type: none"> - Instalacja serwera konsoli EDR na maszynie wskazanej przez Zamawiającego; - Wstępna konfiguracja; - Przygotowanie wstępnych, domyślnych polityk; - Wdrożenie agenta EDR - Sprawdzenie poprawności działania serwera konsoli EDR - Przegląd detekcji zgromadzonych w konsoli - Wspólna analiza i optymalizacja, - Wspólne tworzenie wykluczeń <p>Wymagane jest aby wdrożenie przeprowadzone było przez Inżyniera Wykonawcy, posiadającego certyfikat producenta dostarczanego rozwiązania.</p>	Spełnia / nie spełnia
Ilość	1 szt.	

Część 8 : Pamięć masowa

8.1 – Dyski twarde 3,5 cala

Specyfikacja sprzętu			
Ogólne	Pojemność minimalna.	16 TB	Spełnia / nie spełnia

	Obudowa	3.5"	Spełnia / nie spełnia	
	Interfejs	SATA 6 Gb/s	Spełnia / nie spełnia	
	Rozmiar sektora	512e	Spełnia / nie spełnia	
Wydajność	Prędkość obrotowa	7,200 rpm	Spełnia / nie spełnia	
	Szybkość interfejsu	6.0 Gb/s, 3.0 Gb/s, 1.5 Gb/s	Spełnia / nie spełnia	
	Rozmiar buforu	512 MiB	Spełnia / nie spełnia	
	Maksymalna stała prędkość przesyłu danych (typ.)	262 MiB/s	Spełnia / nie spełnia	
Niezawodność	Średni czas do awarii (MTTF)	2.5 mln godzin	Spełnia / nie spełnia	
	Ocena obciążenia	550 TB przeniesionych danych rocznie	Spełnia / nie spełnia	
	Gwarancja	5 lat	Spełnia / nie spełnia	
	Uwagi		Spełnia / nie spełnia	
Zużycie energii	Napięcie zasilania	12 V ($\pm 10\%$) / 5 V (+10/-7%)	Spełnia / nie spełnia	
	Aktywny tryb bezczynności (typ.)	4.00 W	Spełnia / nie spełnia	
	Losowy odczyt/zapis (4 KB Q1) (typ.)	7.63 W	Spełnia / nie spełnia	
	Uwagi		Spełnia / nie spełnia	
Temperatura	Działa	5°C do 60°C (41°F do 140°F)	Spełnia / nie spełnia	
	Nie działa	-40°C do 70°C (-40°F do 158°F)	Spełnia / nie spełnia	
Wstrząs	Działa	686 m/s ² {70 G} (czas trwania 2 ms)	Spełnia / nie spełnia	
	Nie działa	2450 m/s ² {250 G} (czas trwania 2 ms)	Spełnia / nie spełnia	
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)	Spełnia / nie spełnia	
	Nie działa	29,4 m/s ² {3.0 G} (od 5 do 500 Hz)	Spełnia / nie spełnia	
Wysokość	Działa	-305 metry do 3,048 metry	Spełnia / nie spełnia	
	Nie działa	-305 metry do 12,192 metry	Spełnia / nie spełnia	
Wilgotność względna	Działa	5-90% R.H. (bez kondensacji)	Spełnia / nie spełnia	
	Nie działa	5-95% R.H. (bez kondensacji)	Spełnia / nie spełnia	
Inne	Rozmiar (wys. x szer. x gł.)	26.1 mm x 101.85 mm x 147 mm	Spełnia / nie spełnia	
	Masa	720 g	Spełnia / nie spełnia	
	Certyfikaty	CE		Spełnia / nie spełnia
		EAC		Spełnia / nie spełnia
		BSMI		Spełnia / nie spełnia
RCM			Spełnia / nie spełnia	

		KC	Spełnia / nie spełnia
		RoHS	Spełnia / nie spełnia
		ICES	Spełnia / nie spełnia
		TUV	Spełnia / nie spełnia
		UL	Spełnia / nie spełnia
	Zgodność.	Zgodność i wsparcie sprzętowe Synology DS1621xs+ lub równoważne .	Spełnia / nie spełnia
Licencje / Ilość	Zamawiający dostarczy ww. produkt w ilości 4 sztuk		Spełnia / nie spełnia

Część 8.2 : Dyski SSD m2

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

			Spełnia / nie spełnia
	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	Spełnia / nie spełnia
	Średni czas do awarii (MTBF)	1.8 mln godzin	Spełnia / nie spełnia
	UBER (bitowa stopa nienaprawialnych błędów)	< 1 sector per 10 ¹⁷ bits read	Spełnia / nie spełnia
	Zabezpieczenie przed utratą zasilania	-	Spełnia / nie spełnia
	Gwarancja*	5 lat	Spełnia / nie spełnia

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

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

Część 9 : Licencje MacSec

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