OPIS PRZEDMIOTU ZAMÓWIENIA

Macierz z de-duplikacją dedykowana do backupu i archiwizacji danych

Lp.	Wymagania minimalne
1.	Przedmiotem zamówienia jest dostarczenie urządzenia do backupu danych i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli.
2.	Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania. System do kopii zapasowych musi być integralną częścią macierzy.
3.	Oferowane urządzenie musi być fabrycznie nowe, wyprodukowane najwcześniej w roku 2023 i pochodzić z autoryzowanego kanału dystrybucji producenta oraz nie może być zarejestrowane na żadnego innego klienta końcowego. Urządzenie wraz z oprogramowaniem musi być objęte wsparciem serwisowym producenta przez okres zadeklarowany w ofercie - nie mniejszy niż 36 miesięcy w trybie 24/7 z czasem reakcji na poziomie NBD (Next Business Day) dla sprzętu oraz oprogramowania. W okresie wsparcia serwisowego wymagane jest bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii, dostęp na portalu producenta do najnowszych wersji oprogramowania sprzętowego. Uszkodzone dyski pozostają u Zamawiającego bez ponoszenia dodatkowych kosztów. Zgłaszanie oraz obsługa awarii musi być możliwa poprzez portal producenta na koncie Zamawiającego.
4.	Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe: Obudowa rack 19” rozmiar 2U Pamięć RAM: 128 GB Osobne dyski M2 działające w RAID w celu instalacji warstwy oprogramowania i systemu operacyjnego, Redundantne zasilanie, Gwarancja NBD on-premise o czasie trwania analogicznym do trwania wsparcia technicznego.
5.	Oferowane urządzenie musi posiadać pojemność co najmniej 120TB netto (powierzchni użytkowej widocznej po założeniu systemu plików) bez uwzględniania mechanizmów protekcji – przestrzeń dedykowana do gromadzenia de-duplikatów. W ramach oferowanego urządzenia wymagane jest skalowanie do maksymalnej pojemności co najmniej 200 TB netto (powierzchni użytkowej widocznej po założeniu systemu plików). Rozbudowa nie może pociągać konieczności dołożenia dodatkowych kontrolerów oraz półek z dyskami, nie może być również realizowana poprzez zwielokrotnienie ilości oferowanych urządzeń.
6.	Oferowane urządzenie musi umożliwiać jednoczesny dostęp protokołami HTTPS oraz S3.

7.	Oferowane urządzenie musi umożliwiać rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityka retencyjną), powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę, wymagane wsparcie dla dla AWS, Microsoft Azure oraz Google GCP. Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń co najmniej 340TB netto dla warstwy CLOUD.
8.	Oferowane urządzenie musi posiadać minimum: ● 4 porty Ethernet 10Gb/s BaseT ● 4 porty Ethernet 10Gb/s SFP+ (wymagana pełna obsada wkładek) wymagana możliwość obsługi każdym z w/w portów protokołów CIFS, NFS, de-duplikacja na źródle Oferowane urządzenie musi umożliwiać rozbudowę, o co najmniej (bez konieczności usuwania w/w portów Ethernet) ● 2 porty FC 16Gb/s wymagana możliwość obsługi poprzez porty FC oraz de-duplikacja na źródle.
9.	Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, de-duplikacja na źródle, VTL dla oferowanej pojemności urządzenia
10.	Produkt musi być dostępny w polskiej wersji językowej.
11.	Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter powinno być zlokalizowane na terenie Polski)
12.	Konsola zarządzająca musi być dostępna z poziomu przeglądarki internetowej.
13.	System musi pozwalać na automatyczne aktualizacje oprogramowania.
14.	Oprogramowanie do zarządzania musi rezydować na oferowanym urządzeniu.
15.	Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
16.	Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
17.	Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
18.	Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
19.	Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.
20.	Urządzenie musi mieć możliwość zarządzania poprzez Interfejs graficzny dostępny z przeglądarki internetowej oraz poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)

21.	Wymagana funkcjonalność Load Balancing dla oprogramowania backupowego oraz Link Failover dla sprzętu.
22.	System zarządzania nie może być oparty o relacyjne bazy danych.

23.	System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków, plików i folderów.
24.	System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
25.	System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia.
26.	System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
27.	System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
28.	Wymagane wsparcie dla backupów typu Virtual Synthetics.
29.	Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych: ● actidata actiLib LTO Family ● ADIC Scalar Series ● BDT FlexStor II, MultiStak and MultiStor ● Cristie GigaStream T Series ● Fujitsu Eternus Series ● HP/HPE MSL Series ● IBM TS Series ● Overland-Tandberg NEO Series ● Qualstar Q Series ● Quantum Scalar Series ● Spectra Logic T Series
30.	Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7
31.	W przypadku de-duplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
32.	System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
33.	Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.
34.	Urządzenie musi umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia.
35.	Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.

36.	Technologia deduplikacji musi wykorzystywać algorytm bazujący na stałym bloku, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
37.	Urządzenie musi wspierać de-duplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych: ● Windows ● Linux (RedHat, SuSE)
38.	Oferowany produkt musi posiadać obsługę mechanizmów globalnej de-duplikacji dla danych przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) również powinny składować dane zdeduplikowane.
39.	Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.
40.	Proces deduplikacji musi odbywać się in-line – po stronie źródła przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. Wymaganie de- duplikacji in-line dotyczy zapisu danych przez każdy z wymaganych interfejsów.
41.	Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej de-duplikacji (wymagana de-duplikacja in-line)

42.	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
43.	Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
44.	Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
45.	Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.
46.	Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymaganie dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych.
47.	System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
48.	Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: RMAN, Microsoft SQL Server Management Studio. W przypadku współpracy z każdą z poniższych aplikacji:

	● RMAN (dla ORACLE) ● Microsoft SQL Server Management Studio (dla Microsoft SQL) urządzenie musi umożliwiać de-duplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. De-duplikacja w wyżej wymienionych przypadkach musi zapewniać aby do oferowanego urządzenia były transmitowane poprzez sieć – LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu.
49.	W przypadku przyjmowania backupów z Oracle RMAN oraz Microsoft MSSQL, urządzenie musi umożliwiać de-duplikację na źródlei przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC. De-duplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwerów do urządzenia były transmitowane poprzez sieć FC tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu.
50.	Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia (bez pośrednictwa dodatkowych modułów) takiego samego typu oraz innych, wspierających technologię CIFS, NFS, S3, iSCSI. Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację na oferowane urządzenie musi być dostarczona w ramach niniejszego postępowania.
51.	Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.
52.	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
53.	W przypadku replikacji danych między dwoma urządzeniami, muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności: ● replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących ● replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu ● replikacja zarządzana jest z poziomu wymaganej aplikacji ● aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji
54.	Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami oferowanego typu – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji.
55.	System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
56.	System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.

57.	Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
58.	Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
59.	System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
60.	Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych
61.	Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.
62.	System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
63.	System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
64.	Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
65.	Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.
66.	System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika.
67.	Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
68.	Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.
69.	Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).
70.	System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
71.	System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system

	musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.
72.	Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
73.	Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
74.	W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.
75.	Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
76.	System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
77.	System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
78.	System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental
79.	Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.
80.	Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)
81.	Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.
82.	Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu)
83.	Dla środowisk fizycznych i baz danych: 1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami. 2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń. 3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej. 4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.

	5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji. 6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych. 7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux. 8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem. 9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika. 10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych. 11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V. 12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK). 13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych. 14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).
84.	Dla środowisk wirtualnych: 1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów. 2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych. 3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych. 4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner. 5. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware

	oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych. 6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna). 7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere. 8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.
85.	Dla aplikacji SaaS: 1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza. 2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji) 3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365. 4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi 5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe. 6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git. 7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium. 8. System musi umożliwiać zabezpieczenie środowisk Jira 9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.
86.	System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").
87.	System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System
88.	System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.
89.	W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowały działanie Systemu. System nie może posiadać pojedynczego punktu awarii.
90.	System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w

	konfiguracji agenta na zabezpieczonym urządzeniu.