

Opis Przedmiotu Zamówienia (OPZ)
na dostawę subskrypcji oprogramowania rozwiązań Veeam (lub rozwiązań równoważnych)
na okres 3 lat, wraz z usługą wdrożenia oprogramowania oraz szkoleniem administratorów

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest:

L.p.	Nazwa produktu	Numer katalogowy	Licencjonowanie	Ilość
1.	Dostawa subskrypcji oprogramowania: Veeam Backup for Microsoft Office 365. 3 Years Subscription Upfront Billing & Production (24/7) Support. Public Sector.	P-VBO365-0U-SU3YP-00	Per user	1430 users
2.	Dostawa subskrypcji oprogramowania: Veeam Availability Suite Universal Subscription License. Includes Enterprise Plus Edition features. 3 Years Subscription Upfront Billing & Production (24/7) Support. Public Sector.	P-VASVUL-0I-SU3YP-00	Per virtual machine	60 vm
3.	Usługa wdrożenia oprogramowania w infrastrukturze Zamawiającego, w tym wykonanie testów powdrożeniowych	---	---	---
4.	Usługa szkolenia administratorów Zamawiającego, w siedzibie Zamawiającego, w zakresie zarządzania oprogramowaniem wymienionym w pkt 1 i 2	---	---	5 administratorów

Dostarczone oprogramowanie musi posiadać centralną konsolę zarządzania. Konsola zarządzania musi pozwalać na zarządzanie nieograniczoną ilością licencji oprogramowania wskazanego w pkt 1 i 2 przedmiotu zamówienia (Zamawiający przewiduje rozbudowę systemu).

Dostarczone oprogramowanie musi posiadać wsparcie serwisowe realizowane przez producenta lub dostawcę oprogramowania na czas nie krótszy niż 36 miesięcy od dnia dostawy oprogramowania.

Dostarczone oprogramowanie musi pochodzić z oficjalnego kanału dystrybucyjnego producenta. Zamawiający dopuszcza dostawę oprogramowania równoważnego, po spełnieniu wymagań minimalnych określonych poniżej.

II. SPOSÓB REALIZACJI

- Subskrypcje muszą zostać zarejestrowane na Urząd Marszałkowski Województwa Mazowieckiego w Warszawie. Dostawca oprogramowania przekaze odpowiedni certyfikat licencyjny lub inny dokument, który jednoznacznie potwierdzi taką rejestrację, ilość pozyskanych licencji oraz okres obowiązywania subskrypcji.
- Dostawca wykona wdrożenie oprogramowania w infrastrukturze Zamawiającego, polegające na m.in. instalacji oprogramowania, konfiguracji oprogramowania, uruchomieniu oprogramowania, przeprowadzenia testów powdrożeniowych. Prace wdrożeniowe muszą zostać wykonane przez osoby posiadające kompetencje potwierdzone certyfikatem Veeam Certified Engineer lub Veeam Certified Architect. Zamawiający wymaga dostarczenia kopii certyfikatów na potwierdzenie posiadanych kompetencji.
- Dostawca wykona szkolenie dla wskazanej liczby administratorów Zamawiającego. Szkolenie powinno być przeprowadzone przez trenera posiadającego kompetencje potwierdzone certyfikatem Veeam Certified Engineer lub Veeam Certified Architect. Zamawiający nie oczekuje szkolenia certyfikowanego. Zakres szkolenia musi zawierać zarządzanie oprogramowaniem we wszystkich funkcjonalnościach niezbędnych do samodzielnej eksploatacji oprogramowania. Szkolenie powinno zostać zrealizowane w siedzibie Zamawiającego (Warszawa). Dopuszcza się realizację w formule zdalnej (online) z wykorzystaniem narzędzi komunikacyjnych, umożliwiających pełną interakcję trenera z uczestnikami.

III. ROZWIĄZANIA RÓWNOWAŻNE

Oferowane rozwiązanie równoważne musi znaleźć się w czołówce raportu Gartner Magic Quadrant for Data Center Backup and Recovery Solutions. Dodatkowo musi znajdować się na liście referencyjnej Gartner <https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions> z minimalnym wymogiem 150 referencji i minimalnym wynikiem 4,5 punktów.

WYMAGANIA MINIMALNE DLA OPROGRAMOWANIA RÓWNOWAŻNEGO DLA PRODUKTU WYMIENIONEGO W PKT1 PRZEDMIOTU ZAMÓWIENIA

WYMAGANIA	
1.	Rozwiązanie musi wykonywać kopię zapasową danych Microsoft Exchange Online w ramach usługi Office365 oraz lokalnych instancji Microsoft Exchange
2.	Rozwiązanie musi wykonywać kopię zapasową danych Microsoft Sharepoint Online w ramach usługi Office365 oraz lokalnych instancji Microsoft Sharepoint
3.	Rozwiązanie musi wykonywać kopię zapasową danych Microsoft OneDrive for Business w ramach usługi Office365
4.	Rozwiązanie musi wykonywać kopię zapasową danych Microsoft Teams w ramach usługi Office365
5.	Rozwiązanie musi pozwalać na dodanie wielu subskrypcji Office365 oraz wielu lokalnych serwerów Exchange oraz Sharepoint.
6.	Rozwiązanie nie może instalować żadnych agentów po stronie lokalnych instancji Exchange oraz Sharepoint. Wymaga się wykorzystania API wewnętrznych aplikacji.
7.	Rozwiązanie nie może wymagać tworzenia dodatkowych elementów/agentów po stronie Office365.
8.	Rozwiązanie nie może dodawać żadnych dodatkowych kont członkowskich do zabezpieczanych grup będących częścią zespołów MS Teams.
9.	Rozwiązanie musi wspierać uwierzytelnianie wieloskładnikowe (MFA)
10.	Rozwiązanie musi być licencjonowane per użytkownik.
11.	Rozwiązanie musi być licencjonowane w modelu subskrypcyjnym.
12.	Rozwiązanie musi posiadać skalowalną architekturę (serwer zarządzający, repozytorium). Nie dopuszcza się, aby komponenty systemu backupu były dodatkowo licencjonowane.
13.	Rozwiązanie musi przechowywać dane w macierzystym formacie Microsoft Exchange.
14.	Rozwiązanie musi pozwolić przechowywać dane na lokalnych zasobach lub na zasobach obiektowych (Microsoft Azure Blob, AWS S3 bucket oraz innych kompatybilnych z protokołem S3)
15.	Rozwiązanie musi pozwalać na granularne odzyskiwanie dowolnych elementów Microsoft Exchange (skrzynka, mail, kontakt, wpis z kalendarza, element folderu „Permanently Deleted Items”).
16.	Rozwiązanie musi pozwalać na granularne odzyskiwanie dowolnych elementów Microsoft Sharepoint. Opcja odtworzenia elementów, witryn.
17.	Rozwiązanie musi pozwalać na granularne odzyskiwanie dowolnych elementów Microsoft OneDrive. Opcja odtworzenia plików, folderów lub całych kont OneDrive
18.	Rozwiązanie musi pozwalać na granularne odzyskiwanie dowolnych elementów Microsoft Teams. Opcja odtworzenia całych zespołów, kanałów, zakładki, plików oraz konwersacji.
19.	Rozwiązanie musi pozwalać na odzysk elementów do skrzynki w pakiecie Office 365, lokalnej skrzynki Exchange, pliku oraz w formacie PST.
20.	Rozwiązanie musi pozwalać na hybrydowe scenariusze backupu/odzysku (np. backup wykonany z lokalnej instancji Exchange, odzysk do Exchange Online w Office365)
21.	Rozwiązanie musi pozwalać na granularne przeszukiwanie zabezpieczonych danych (eDiscovery)
22.	Rozwiązanie musi mieć możliwość integracji z innymi rozwiązaniami poprzez PowerShell oraz RESTful API.
23.	Rozwiązanie musi posiadać możliwość skonfigurowania audytu dla wybranych obiektów (np. dla skrzynki mailowej). Próba przeglądania, odtwarzania tych danych spowoduje wysłanie maila do audytora.

WYMAGANIA MINIMALNE DLA OPROGRAMOWANIA RÓWNOWAŻNEGO DLA PRODUKTU WYMIENIONEGO W PKT 2 PRZEDMIOTU ZAMÓWIENIA

WYMAGANIA OGÓLNE	
1.	Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2012, 2012 R2, 2016 oraz 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
2.	Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
3.	Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
4.	Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
WYMAGANIA DOTYCZĄCE ARCHITEKTURY	
5.	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
6.	Oprogramowanie musi tworzyć "samowystarczalne" archiwa, do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków

7.	Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-incremental)
8.	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
9.	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.
10.	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.
11.	Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
12.	Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
13.	Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
14.	Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
15.	Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
16.	Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
17.	Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
18.	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
19.	Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
20.	Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
21.	Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
WYMAGANIA DOTYCZĄCE WYKONYWANIA KOPII ZAPASOWYCH	
22.	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
23.	Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczeniu udziałów plikowych.
24.	Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
25.	Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru
26.	Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
27.	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 i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage.
28.	Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
29.	Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
30.	Oprogramowanie musi posiadać wsparcie dla NDMP
31.	Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
32.	Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
33.	Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
34.	Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
35.	Repozytoria oparte o XFS muszą pozwalać na zmieszanie danych przez określoną ilość czasu (tzw Immutability)

36.	Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
37.	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.
38.	Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAAI, 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.
39.	Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
40.	Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
41.	Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
WYMAGANIA DOTYCZĄCE ODTWARZANIA KOPII ZAPASOWYCH	
42.	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 oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
43.	Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
44.	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
45.	Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere
46.	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
47.	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
48.	Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
49.	Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
50.	Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików: <ul style="list-style-type: none"> • Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs • BSD: UFS, UFS2 • Solaris: ZFS, UFS • Mac: HFS, HFS+ • Windows: NTFS, FAT, FAT32, ReFS • Novell OES: NSS
51.	Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
52.	Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
53.	Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
54.	Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
55.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
56.	Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
57.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2012 i nowszych
58.	Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
59.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych
60.	Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
61.	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.
62.	Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
63.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
64.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA
65.	Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
WYMAGANIA DOTYCZĄCE WERYFIKACJI KOPII ZAPASOWYCH	
66.	Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.

67.	Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
68.	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
69.	Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
70.	Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
71.	Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
WYMAGANIA DOTYCZĄCE MONITOROWANIA	
72.	System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
73.	System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsolę vCenter Server lub pracujące samodzielnie
74.	System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
75.	System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware
76.	System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
77.	System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
78.	System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
79.	System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
80.	System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
81.	System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
82.	System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
83.	System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
84.	System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
85.	System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
86.	System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
87.	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 supportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
88.	System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware
89.	System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 8.x i 9.x
WYMAGANIA DOTYCZĄCE RAPORTOWANIA	
90.	System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2012, 2012 R2, 2016 oraz 2019
91.	System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
92.	System musi być certyfikowany przez VMware i posiadać status „VMware Ready”
93.	System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
94.	System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
95.	System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
96.	System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
97.	System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów

98.	System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
99.	System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
100.	System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
101.	System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
102.	System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
103.	System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.
104.	System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware
105.	System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
106.	System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie
DODATKOWE WYMAGANIA FUNKCJONALNE	
107.	Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
108.	Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
109.	Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
110.	Rozwiązanie musi wspierać systemy operacyjne macOS
111.	Rozwiązanie musi wspierać wykonywanie kopii zapasowych następujących systemów plików: NTFS, ReFS, FAT32, ext2, ext3, ext4, ReiserFS, JFS, XFS, F2FS, Brfs (dla kernela 3.16 i nowszych), APFS, HFS, HFS+, NILFS2
112.	Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
113.	Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
114.	Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów oraz wybranych plików i folderów
115.	Rozwiązanie musi wspierać backup podłączonych dysków USB
116.	Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
117.	Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na: <ul style="list-style-type: none"> • 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 Chmury • Zcentralizowanym repozytorium danych
118.	Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
119.	Rozwiązanie musi wspierać kontrolę pasma sieciowego
120.	Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
121.	Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
122.	Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
123.	Rozwiązanie musi wspierać skrypty wykonywane przed i po wykonaniu zadania oraz przed i po wykonaniu migawki na poziomie wolumenu.
124.	Rozwiązanie musi wspierać technologię BitLocker
125.	Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
126.	Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla: <ul style="list-style-type: none"> • Microsoft Exchange 2013 i nowszych • Microsoft Active Directory 2012 i nowszych • Microsoft Sharepoint 2013 i nowszych • Microsoft SQL 2012 i nowszych • Oracle 11g i nowszych
127.	Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
128.	Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL poprzez bezpośrednie uruchomienie ich z pliku backupu.

129.	Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2
130.	Rozwiązanie musi wspierać szyfrowanie
131.	Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
132.	Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczonego
133.	Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
134.	Rozwiązanie musi wspierać tworzenie wielu zadań backupowych