Opis przedmiotu zamówienia

Dostawa i wdrożenie systemu backupu i archiwizacji danych

1. Zarządzanie i magazyny danych

1.1. Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2024

1.2. System powinien być dostarczony w ramach urządzenia sprzętowego z zainstalowanymi i skonfigurowanymi wszystkimi usługami niezbędnymi do prawidłowej pracy systemu.

1.3. Zaproponowane urządzenie musi spełniać minimalne poniższe wymagania sprzętowe:

1.3.1. obudowa rack 2U,

1.3.2. procesor: min. 8 rdzeni, min. 16 wątków. Minimalna częstotliwość bazowa procesora 2.8GHz,

1.3.3. pamięć RAM minimum 32GB DDR4,

1.3.4. przestrzeń dostępna na przechowywanie danych min. 60TB w konfiguracji RAID6 (całkowita przestrzeń dyskowa min. 120TB),

1.3.5. dodatkowo dyski SSD M.2 nVME działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego,

1.3.6. redundantne zasilanie,

1.3.7. interfejsy sieciowe min. 2 szt. Ethernet 1Gb, Dual SFP+,

1.3.8. gwarancja Next Business Day (NBD) realizowana na miejscu o czasie trwania analogicznym do trwania wsparcia technicznego dla oprogramowania.

1.4. Produkt dostępny w polskiej wersji językowej.

1.5. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej.

1.6. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków.

1.7. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów.

1.8. System musi umożliwiać tworzenie kopii zapasowych do wielu lokalizacji docelowych.

1.9. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT.

1.10. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft.

1.11. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe.

1.12. System zarządzania nie może być oparty o relacyjne bazy danych.

1.13. Rozwiązanie musi działać w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia lub odzyskiwania kopii zapasowej).

1.14. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług oraz urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów.

1.15. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, żaden inny element Systemu nie powinien brać udziału w przesyłaniu danych.

1.16. Rozwiązanie musi umożliwiać tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.

1.17. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.

1.18. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
1.19. 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.
1.20. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
1.21. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
1.22. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
1.23. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych.
1.24. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów wstępnych i końcowych oraz po wykonaniu migawki VSS.
1.25. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
1.26. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualne, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
1.27. 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.
1.28. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail o statusie wykonywanych zadań na dowolne adresy podane przez użytkownika w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.
1.29. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, replikacja, testowe odtwarzanie maszyn wirtualnych).
1.30. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.
1.31. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
1.32. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych zdeduplikowanych.
1.33. 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.
1.34. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
1.35. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.

1.36. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
1.37. Konfiguracja, modyfikacja ustawień polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
1.38. System musi pozwalać na automatyczne aktualizacje oprogramowania.
1.39. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
1.40. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia.
1.41. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność, dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.
1.42. System będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
1.43. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracane dane.
1.44. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
1.45. System musi pozwalać na gradację uprawnień administratorów - umożliwiać 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.
1.46. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu w momencie spełnienia dodatkowych wymogów.
1.47. 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.
1.48. 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.
1.49. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
1.50. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
1.51. System powinien posiadać predefiniowane schematy tworzenia kopii zapasowych, min. Custom, Basic, GFS, Forever incremental.
1.52. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
1.53. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych producenta urządzenia zlokalizowana na terenie Polski.
1.54. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, S3, nfs, iscsi, katalog lokalny.
1.55. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa.
1.56. 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.

1.57. Możliwość generowania raportów dobowych w oparciu o harmonogram.

1.58. 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).

1.59. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, system operacyjny, adres IP.

1.60. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu).

2. Wspierane systemy

2.1. Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach Docker opartych o systemy:

2.1.1. Debian 9+,

2.1.2. Ubuntu 17+,

2.1.3. RHL 6+,

2.1.4. Windows 7, 8.1, 10, 11,

2.1.5. Windows Server 2008 R2+,

2.2. Środowiskach wirtualnych

2.2.1. Hyper-V 2016+,

2.2.2. Vmware 6.7+.

3. **Środowiska fizyczne i bazy danych**

3.1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.

3.2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.

3.3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.

3.4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.

3.5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.

3.6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych.

3.7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.

3.8. 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.

3.9. 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.

3.10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.

3.11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.

3.12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).

3.13. 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.

3.14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).

4. Środowiska wirtualne

4.1. System musi wspierać kopię w trybie świadomy aplikacji (application-aware) dla wszystkich wspieranych wirtualizatorów.

4.2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowaniem zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.

4.3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.

4.4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.

4.5. 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 Hyper-V oraz Vmware niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.

4.6. Dla środowiska Hyper-V i vSphere rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).

4.7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.

4.8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.

5. Licencjonowanie i wsparcie techniczne

5.1. Wszystkie linie wsparcia muszą być obsługiwane w języku polskim.

5.2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.

5.3. Możliwość zgłaszania problemów bezpośrednio z poziomu interfejsu zarządzania w formie czatu.

5.4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów).

5.5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu zgłoszeniowego oraz wsparcia telefonicznego.

5.6. W ramach wsparcia technicznego Zamawiający musi mieć dostęp do osoby dedykowanej po stronie Dostawcy do obsługi zgłoszeń technicznych, doraźnej pomocy i bieżącej pomocy w utrzymania infrastruktury Zamawiającego.

5.7. W ramach dokumentacji posprzedażowej Dostawca musi dostarczyć bezpośredni numer telefonu oraz adres e-mail do osoby dedykowanej po stronie Dostawcy.

5.8. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych.

5.9. Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu.

5.10. Wsparcie techniczne producenta na oprogramowanie musi zostać dostarczone na min. 36 miesięcy.

5.11. Licencje powinny umożliwiać replikacje na własne zasoby.

5.12. Wymagane oświadczenie producenta, że dla zakupionego produktu (warstwa sprzętowa) będzie wspierana minimum 7 lat od momentu zamówienia. Jeśli okaże się to niemożliwe producent będzie zobowiązany do migracji warstwy sprzętowej na nowszą przy zachowaniu ciągłości wsparcia technicznego.

6. Anty-ransomware i bezpieczeństwo

6.1. 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").

6.2. System powinien umożliwiać wykorzystanie wbudowanego menadżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System.

6.3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.

6.4. 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 sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.

6.5. 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 zabezpieczanym urządzeniu.

7. Wdrożenie

7.1. Zamawiający dopuszcza wdrożenie i szkolenie w formule zdalnej.

7.2. Wdrożenie zdalne musi być realizowane bezpośrednio przez producenta oferowanego systemu backupowego.

7.3. Wdrożenie musi zostać przeprowadzone przez dedykowanego inżyniera od producenta systemu backupowego.

7.4. Wdrożenie musi zakończyć się dostarczeniem dokumentacji powdrożeniowej, przygotowanej przez dedykowanego inżyniera od producenta systemu backupowego.

7.5. Zamawiający może skorzystać z przynajmniej 8h pomocy wdrożeniowej bezpośrednio świadczonej przez producenta rozwiązania.

7.6. Wdrożenie powinno być zrealizowane tak, aby dostosować się do preferencji zamawiającego.