Otwock, 21.12.2020 r.

Nr sprawy: 34/W/2020

Dotyczy: **Dostawy rozwiązania do przechowywania danych backupu wraz z ich deduplikacją i ochroną Ramsomware.**

W związku z pytaniami do niniejszego postępowania, Zamawiający udziela dodatkowych wyjaśnień :

Pytanie 1.

Zamawiający w dokumencie „Przetarg wew dzial DS_06_2020_pod.pdf" w Wymaganiach Technicznych w pkt 2 i 3 napisał:
„2. Rozwiązanie musi umożliwiać zapis danych z wydajnością nie niższą niż 2.4TB/godz. bez obciążania zewnętrznych serwerów (klientów) procesem deduplikacji. Wydajność ta musi być potwierdzona dokumentacją producenta.

3. Rozwiązanie musi umożliwiać przewidywalny oraz krótki czas odtwarzania przez przechowywanie wybranych kopii zapasowych w formie niezdeduplikowanej. Wymagana przestrzeń na dane niezdeduplikowane powinna wynosić minimum 10TB. W przypadku jeżeli oferowane rozwiązanie nie posiada dedykowanej przestrzeni na dane niezdeduplikowane dopuszczalne jest dostarczenie wymaganej, dodatkowej przestrzeni w postaci drugiego urządzenia o pojemności minimum 10TB i wydajności minimum 2.4TB/h „

Wymóg powyżej wymusza jedną niewyrafinowaną metodę realizacji celu biznesowego i technicznego jakim jest przewidywalne i krótkie odtworzenie. Nadmieniamy, że takie rozwiązanie jest stosowane jedynie przez bardzo niewielu producentów rozwiązań.

Liderzy rynkowi, dysponują technologią, w której przestrzenie na tzw. stage'ing są zbędne przy wydajności odtworzenia na poziomie 5TB/h oraz backup na poziomie do 10-14TB/h dla urządzeń, o pojemności wyspecyfikowanej pkt. 5 – wielokrotnie przekraczających wymagania techniczne z pkt 2 i 3.

Jednocześnie wymóg drugiego urządzenia bez deduplikacji przeczy wymaganiom z punktu 7 o przesyłaniu wyłącznie niezdeduplikowanych danych przez sieć WAN.

Wymóg w obecnym brzmieniu preferuje i ogranicza rozwiązania do technologii, które nie zawierają w sobie najnowszych technologii i które nie spełniają najwyższych obecnie standardów na rynku. Wymóg w obecnym brzmieniu preferuje technologie, które:

1. wymagają zwiększenia przestrzeni do destagingu każdorazowo przy zwiększeniu pojemności dziennego backupu pod rygorem drastycznego spadku wydajności tworzenia kopii zapasowych.

2. replikacja do drugiego ośrodka jest odsunięta w czasie do zakończenia się procesu deduplikacji na lokalnym urządzeniu – wielokrotne pogorszenie parametru RPO dla drugiej lokalizacji/DC.

3. zabezpieczenie przestrzeni typu staging jest gorsze – zwykle nie gwarantuje odporności na awarię 2+ dowolnych dysków.

Nadmieniamy, że nawet większość nowoczesnych macierzy dyskowych wiodących producentów z czołówki raportów typu Gartner / Forrester wspiera deduplikację i kompresję w locie (czyli bez przestrzeni typu staging) dla macierzy produkcyjnych klasy Enterprise, T0 i T1 – a nie wyłącznie dla dedykowanych urządzeń backupowych.

Mając na uwadze powyższe zwracamy się z uprzejmą prośbą o potwierdzenie, że urządzenia o udokumentowanej w ogólnie dostępnej dokumentacji wydajności tworzenia kopii na poziomie 14TB/h oraz odtworzenia na poziomie 5TB/h spełniają wymogi Zamawiającego bez konieczności dostarczenia przestrzeni na niezdeduplikowalne backupy i/lub drugiego urządzenia o pojemności 10TB i wydajności

2,4TB/h, jeśli jednocześnie zapewniają funkcjonalność uruchomienia wirtualnych maszyn wprost z kopii zapasowej.

Odpowiedź:
Jeżeli urządzenie zapewni uruchomienie wirtualnej maszyny wprost z swojego zasobu zdeduplikowanego to spełni wymagania Zamawiającego i nie musi posiadać dodatkowej przestrzeni niezdeduplikowanej.

Pytanie 2.

Zamawiający w dokumencie „Przetarg wew dzial DS_06_2020_pod.pdf" w Wymaganiach Technicznych w pkt 5 napisał:
"Architektura rozwiązania musi umożliwiać rozbudowę do minimum 120 TB pojemności użytkowej netto bez wymiany oferowanych kontrolerów urządzeń"

Zajętość urządzenia zależy od użytych technologii deduplikacji i kompresji danych - generując nawet kilkudziesięciokrotne różnice w zajętości urządzeń różnych dostawców.
Mając na uwadze powyższe, zwracamy się z uprzejmą prośbą o zmianę sformułowania na wymóg możliwości rozbudowy do pojemności zapewniającej ochronę do 80TB danych źródłowych w reżimie opisanym niniejszym Wymaganiach Technicznych pkt. 1., nie mniej jednak niż 100TB pojemności netto. Takie sformułowania zapewni Zamawiającemu bezpieczeństwo inwestycyjne pozwalając na ochronę 8 krotnie większej ilości danych od obecnie posiadanych, zapewniając jednocześnie optymalizację kosztów w obecnym postępowaniu.

Odpowiedź:
Zamawiający nie wyraża zgody na zmianę specyfikacji w tym zakresie.

Doprecyzowanie pytania nr 2.
Mając na uwadze, że technologia redukcji danych używanych przez różnych producentów daje znacząco różne rezultaty np. poziom deduplikacji stałym blokiem o wielkości 128kB pozwala, przy tej samej pojemności netto, ochronić 3 krotnie mniej danych źródłowych od rozwiązania z technologią Dynamicznego Bloku Danych definiowanego jako:
1. zmienna wielkość bloku dostosowana do typu danych,
2. średnia wielkość bloku 4kB,
3. przesuwne okno w celu detekcji zmian w strumieniach danych mniejszych niż minimalna wielkość bloku deduplikacyjnego urządzenia.

Aby SIWZ nie promował zbytnio urządzeń do wyposażonych w podstawowe technologie opisane powyżej, zwracamy się z prośbą o ograniczenie minimalnej pojemności rozbudowy dla urządzeń z udokumentowaną technologią Dynamicznego Bloku Danych do 104TB pojemności netto. Pojemność ta zapewnia 3-6 krotnie większą pojemność efektywną od przywołanych powyżej urządzeń z technologią dużych (64kB+), stałych bloków danych dopuszczonych obecnymi zapisami SIWZ.

Odpowiedź:
Zamawiający nie dopuszcza zmniejszenia minimalnej pojemności rozbudowy dla urządzeń.

Pytanie 3.
Zamawiający w dokumencie „Przetarg wew dzial DS_06_2020_pod.pdf" w Wymaganiach Technicznych w pkt 6 napisał:
„Rozwiązanie musi posiadać wewnętrzną ochronę przed zmianami danych w backupie (Ransomware) działanie tej funkcji musi być potwierdzone przez producenta. „

Mając na uwadze:
1. Urządzenia oferujące zabezpieczenia migawkami nie pozwalają na automatyczną integrację oprogramowania backupowego z taką funkcjonalnością sprawiając, że rzeczywista ich skuteczność jest zerowa.

2. Ręczna integracja pozostawia okno, w którym oprogramowanie typu ransomware może uszkodzić dane – zerowa skuteczność takiego rozwiązania.

Prosimy o jednoznaczne wskazanie przez Zamawiającego wymaganej technologii mającej zapewnić skuteczność ochrony przed Ransomware czyli np. WORM z granulacją pojedynczego obiektu i retencją ustawianą po zamknięciu obiektu (zakończenia procesu backupu). Nadmieniamy, ze wiodący producenci oprogramowania CommVault, Veeam, VERITAS a także MicroFocus, Dell Quest i inni wspierają tą funkcjonalności w trybie emulacji VTL oraz deklarują integrację z tą funkcjonalnością w najbliższym czasie w dedykowanych interfejsach OST, Catalyst, DDBoost itp. Takie rozwiązanie dostarcza rzeczywistej ochrony oraz przez integrację z oprogramowaniem backupowym zapewnia pełną integrację procesu wykluczając m.inn. pomyłkę ludzką.

Odpowiedź:
Ochrona musi zabezpieczyć dane w okresie wyznaczonego czasu bez możliwości ich modyfikacji i kasowania.

Pytanie 4.
Zamawiający w dokumencie „Przetarg wew dzial DS_06_2020_pod.pdf" w Wymaganiach Technicznych w pkt 8 napisał:
„Proponowane rozwiązanie musi wspierać w ramach jednego systemu następujące metody dostępu:

a. przez LAN z wykorzystaniem protokołów CIFS i/lub NFS
b. przez LAN protokół OST"

Zwracamy uwagę, że udostępnianie danych przez protokoły CIFS i/lub NFS tworzy najprostszy wektor ataku na repozytorium danych systemu backupowego – najbardziej oczywiste wskazanie dla oprogramowania złośliwego.
Zabezpieczenie snapshotami takich zasobów jest funkcją zarządzaną zewnętrznie niezintegrowaną z systemami backup'u – co prowadzi do długotrwałych, ręcznych procedur sprawdzenia poprawności repozytoriów danych oraz czyszczenia metadanych systemu backupowego – procesy te nie gwarantują koherencji oraz implikują same przez siebie utratę danych.
Ograniczenie do protokołu OST nie zapewnia Państwu współpracy z oprogramowaniem Veeam, ComVault, Dell, Quest.

Prosimy o jednoznaczne wskazanie, że nie ograniczają Państwo wsparcia do oprogramowania firmy VERITAS ale urządzenia muszą integrować się z systemami backupu wiodących producentów wymienionych w kwadracie Visionaries i Leaders w publikacji Magic Quadrant firmy Gartner w trybie zapewniającym bezpieczeństwo opisane w punkcie 6 wymagań technicznych oraz, że wymagane do takiej integracji licencje (jeśli konieczne) zostaną dostarczone w ramach obecnego postępowania.

Source: Gartner (October 2019)

Odpowiedź:
Zamawiający potwierdza, że nie ogranicza wymogu wsparcia do oprogramowania wyłącznie firmy VERITAS.

Pytanie 5.
Prosimy o podanie jakiego oprogramowania do wykonywania kopii używa Zamawiający oraz w jakiej wersji celem weryfikacji kompatybilności rozwiązania tj. urządzenie i oprogramowania.

Odpowiedź:
Veeam, MicroFocus.

Pytanie 6.
Prosimy o informację jakiej integracji pomiędzy używanym przez Zamawiającego oprogramowaniem do backupu, a wymaganym rozwiązaniem Zamawiający wymaga (OST, VTL ?).

Odpowiedź:
Sporadycznie NFS, Veeam Data Moover, OST.

Pytanie 7.
Czy Zamawiający wymaga zaoferowania 2 urządzeń do 2 lokalizacji, czy wyłącznie jednego z możliwością rozbudowy w przyszłości o drugie urządzenie ?

Odpowiedź:
Zamawiający wymaga jednego urządzenia.

Pytanie 8.
Czy Zamawiający rozważy dostarczenie w opcji oprogramowania do backupu integrującego się na najwyższym możliwym poziomie z zaproponowanym urządzeniem ?

Jeśli tak prosimy o podanie jakie systemy będą zabezpieczane na urządzeniu z zapytania tj.:

- Ile serwerów fizycznych oraz jakie mają systemy operacyjne, aplikacje/bazy i ile TB danych jest na każdym z nich
- Ile maszyn wirtualnych będzie zabezpieczanych, ile zajmują TB oraz jaka wersję wirtualizatora i licencji posiada Zamawiający
- Czy Zamawiający zamierza zabezpieczać stacje końcowe (laptop/desktop) – jeśli tak to dla ilu użytkowników

Odpowiedź:
Oprogramowanie nie jest przedmiotem zamówienia.

Wszystkie pytania oraz udzielone odpowiedzi stanowią integralną część Załącznika pn: "Przetarg wew dzial DS_06_2020_pod"i są wiążące przy składaniu ofert.