Ulepsz swój plan ochrony danych dzięki szybko działającemu, bardziej niezawodnemu rozwiązaniu do odzyskiwania danych po cyberatakach

Z naszych badań wynika, że rozwiązanie Dell Technologies PowerProtect Cyber Recovery może oferować fizyczną izolację sejfów z kopiami zapasowymi i dokładniejsze skanowanie w celu wykrywania ataków ransomware

Fizyczna izolacja sejfów z kopiami zapasowymi

Tworzenie fizycznej bariery, której dane nie mogą przekroczyć

Dokładniejsze skanowanie w celu wykrywania ataków ransomware

CyberSense analizuje zawartość plików i baz danych, a nie tylko metadane

Skanowanie dwukrotnie większej liczby obciążeń roboczych wykazujących anomalie

Poszukiwanie złośliwego oprogramowania w większej liczbie miejsc za pomocą jednego narzędzia

Średni koszt ataku ransomware wzrósł w ciągu dwóch lat o prawie 20%, do 5,23 mln USD[1]. Skuteczne rozwiązania Cyber Recovery mogą pomóc w zmniejszeniu lub nawet uniknięciu tych potencjalnych kosztów, umożliwiając organizacjom szybkie odzyskiwanie danych po incydentach, ograniczenie utraty danych, zminimalizowanie przestojów, a przy tym zachowanie integralności marki. Rozwiązania powinny dokładnie identyfikować i przywracać dane po ataku do znanego prawidłowego stanu, zapewniając organizacji możliwość odzyskania krytycznych danych i systemów, a jednocześnie pomagając zminimalizować ryzyko biznesowe i przestoje.

Takim rozwiązaniem jest Dell PowerProtect Cyber Recovery (Cyber Recovery). Pomaga ono organizacjom chronić dane i aplikacje przed oprogramowaniem ransomware, destrukcyjnymi cyberatakami i nieoczekiwanymi zdarzeniami. W niniejszym raporcie wykorzystano publicznie dostępne dane w celu porównania podstawowych funkcji ochrony danych i Cyber Recovery z konkurencyjnym rozwiązaniem Rubrik Security Cloud (RSC). W szczególności przyjrzeliśmy się funkcjom, które mogą być ważne dla klientów korzystających z rozwiązań Cyber Recovery, takim jak sejf do odzyskiwania danych, niezmienność, obsługa obciążeń roboczych, technologia skanowania, możliwość odtworzenia i izolacja.

W przeciwieństwie do RSC, rozwiązanie Cyber Recovery wykorzystuje podejście oparte na wielu kopiach, co oznacza, że po utworzeniu kopii zapasowych kopiuje je (a najczęściej ich wybrany podzbiór) do izolowanej pamięci masowej w celu zabezpieczenia i analizy. Rozwiązanie Cyber Recovery składa się z kilku komponentów, w tym z co najmniej jednego sejfu pamięci masowej przechowywanego lokalnie w urządzeniu PowerProtect Data Domain lub w chmurze za pomocą definiowanej programowo pamięci masowej Dell APEX Protection Storage for Public Cloud. Dla porównania, RSC nie oferuje opcji sejfu lokalnego. Cyber Recovery obejmuje też CyberSense, czyli w pełni zautomatyzowany i zintegrowany silnik inteligentnej analizy zabezpieczeń, który skanuje dane, pliki, bazy danych i obrazy w sejfie w poszukiwaniu oznak uszkodzenia w wyniku ataku ransomware. Rozwiązanie CyberSense może skanować dwa razy więcej obciążeń roboczych wykazujących anomalie niż rozwiązanie Rubrik, co może pozwalać CyberSense na skanowanie ML (uczenia maszynowego) w celu wykrycia skutków złośliwego oprogramowania lub innej aktywności cyberprzestępczej w większej ilości danych. Omówimy, w jakim sensie rozwiązanie PowerProtect Cyber Recovery działa inaczej i dlaczego może być bardziej korzystne dla Twojej organizacji.

Przegląd produktu

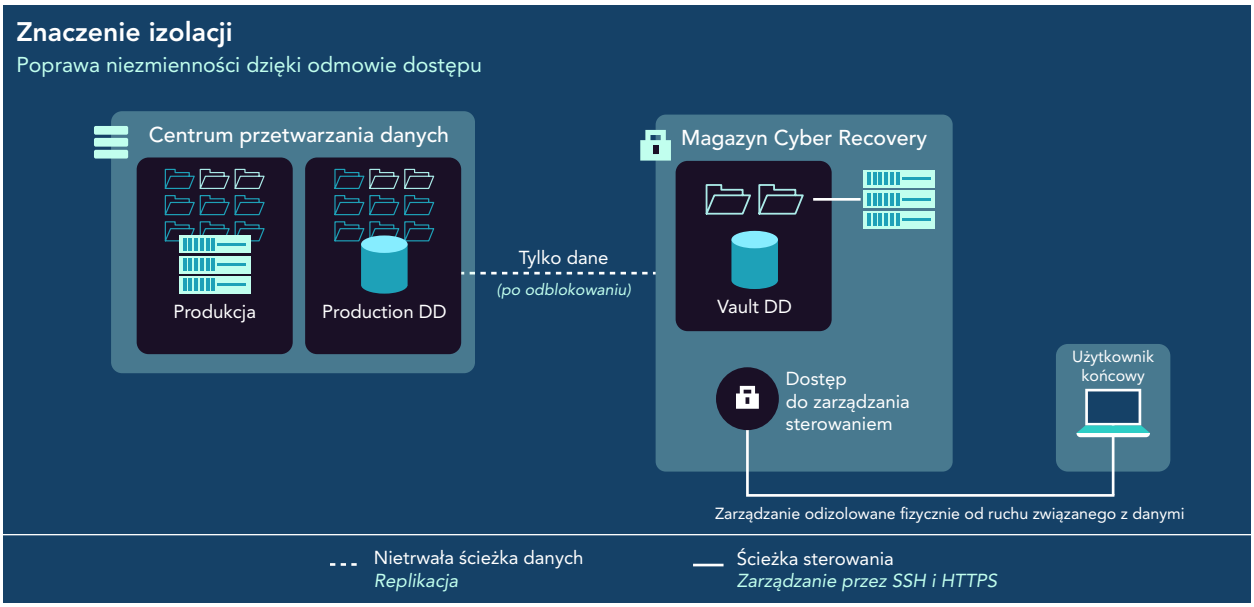
Przegląd rozwiązania Dell PowerProtect Cyber Recovery

Rozwiązanie Dell PowerProtect Cyber Recovery składa się z urządzenia pamięci masowej, w którym przechowywane są dane produkcyjne, oraz docelowego urządzenia pamięci masowej w sejfie na potrzeby replikacji. Obejmuje również oprogramowanie Cyber Recovery, które koordynuje synchronizację, zarządza wieloma kopiami danych w systemie PowerProtect Data Domain (PPDD) umieszczonym w sejfie Cyber Recovery, nadzoruje proces odzyskiwania i nadzoruje proces analizy za pomocą silnika CyberSense.

Rozwiązanie przesyła unikalne dane z produkcyjnej partycji PPDD MTree do jej odpowiednika w sejfie za pośrednictwem replikacji MTree i zapewnia niezmienność danych* przez określony czas. W sejfie znajduje się serwer, który zawiera oprogramowanie Cyber Recovery oraz komponent, w którym rozwiązanie przywraca aplikacje i dane z kopii zapasowych. Każdy sejf Cyber Recovery zazwyczaj zawiera wiele takich komponentów. Sejf zawiera również hosta analitycznego/indeksującego wyposażonego w oprogramowanie do analizy danych, umożliwiając bezpośrednią integrację między oprogramowaniem Cyber Recovery a silnikiem CyberSense.

* Produkty firmy Dell zostały zaprojektowane z myślą o wspieraniu wysiłków klientów na rzecz zabezpieczenia ich danych o znaczeniu krytycznym. Podobnie jak w przypadku każdego produktu elektronicznego, w produktach z zakresu ochrony danych, pamięci masowej i innych elementów infrastruktury mogą występować luki w zabezpieczeniach. Ważne jest, aby klienci instalowali aktualizacje zabezpieczeń zaraz po ich udostępnieniu przez firmę Dell.

Rysunek 1 przedstawia przegląd rozwiązania Dell Cyber Recovery.

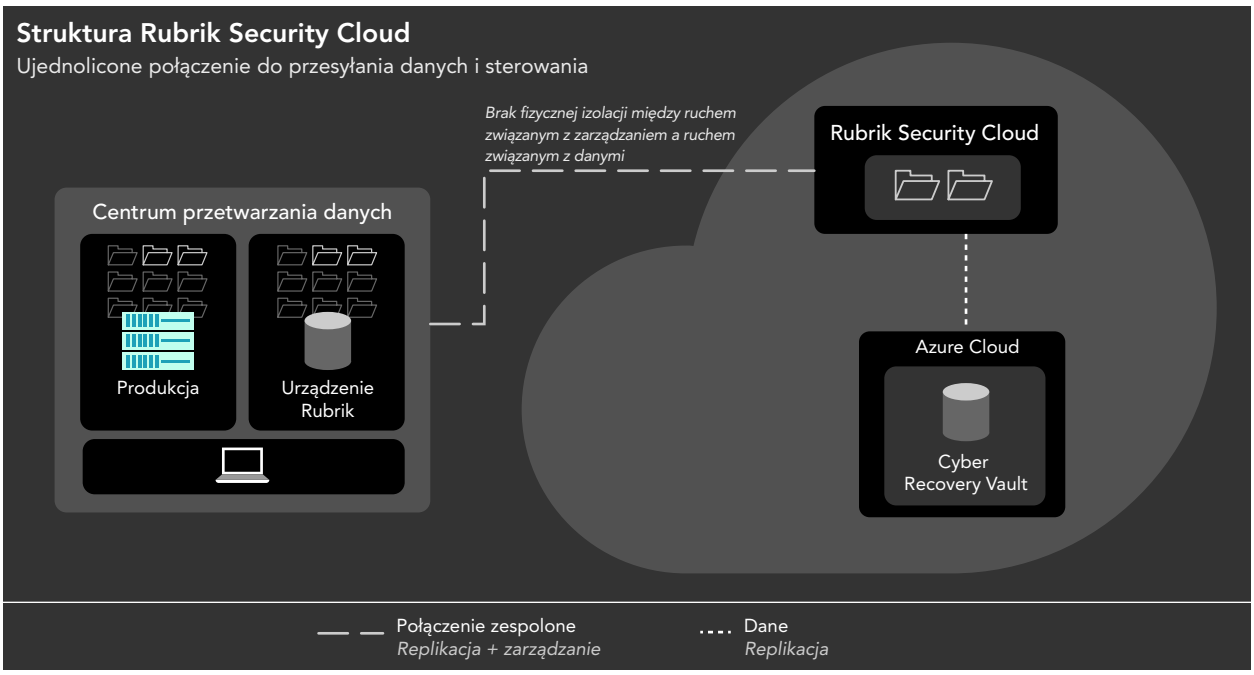


Rysunek 1. Ogólna architektura danych i ścieżki sterowania sejfu Cyber Recovery. Źródło: Principled Technologies.

Aby dowiedzieć się więcej o kluczowych komponentach rozwiązania Dell PowerProtect Cyber Recovery, przeczytaj Przewodnik po rozwiązaniu Dell PowerProtect Cyber Recovery.

Przegląd rozwiązania Rubrik Security Cloud

Firma Rubrik opisuje rozwiązanie Rubrik Security Cloud jako platformę SaaS (software-as-a-service, oprogramowanie jako usługa), która umożliwia klientom „zabezpieczanie danych, monitorowanie ryzyka związanego z danymi i szybkie odzyskiwanie [ich] danych, niezależnie od tego, gdzie się znajdują — w różnych miejscach przedsiębiorstwa, w chmurze czy w aplikacjach SaaS”.[4] Firma Rubrik twierdzi, że zbudowała rozwiązanie w oparciu o „bezpieczną architekturę mikrousług przy użyciu usług o wysokiej dostępności i infrastruktury działającej na platformie Google Cloud Platform (GCP)”.[5] Rysunek 2 przedstawia ogólną strukturę rozwiązania Rubrik Security Cloud.



Rysunek 2. Ogólna struktura rozwiązania Rubrik Security Cloud. Źródło: Principled Technologies.

Obsługa funkcji

Sejf do odzyskiwania danych

Sejfy to dedykowane systemy pamięci masowej, w których przechowywane są zaszyfrowane kopie zapasowe wykonywane przez rozwiązanie w środowisku produkcyjnym. Sejfy nie są częścią produkcyjnych rozwiązań do tworzenia kopii zapasowych. Każdy z nich pełni raczej rolę izolowanej lokalizacji „kopii zapasowej kopii zapasowych", z której klienci mogą odzyskać zweryfikowane kopie zapasowe.

Firma Dell oferuje kilka opcji sejfów, w tym lokalne, w zdalnej kolokacji lub w chmurze publicznej. Sejf lokalny wykorzystuje operacyjne, izolowane fizycznie urządzenie PPDD, które znajduje się w centrum danych, potencjalnie nawet w tej samej szafie, co rozwiązanie do tworzenia kopii zapasowych. Rozwiązanie izolowane fizycznie jest zwykle fizycznie odseparowane od środowiska produkcyjnego. Sejf znajdujący się w zdalnej kolokacji wymaga dedykowanych połączeń sieciowych z sejfem fizycznym, takim jak wersja lokalna, ale jest geograficznie odseparowany w zdalnym centrum danych. Firma Dell udostępnia również sejfy w chmurze publicznej, we współpracy z dostawcami usług w chmurze Amazon Web Services (AWS), Microsoft Azure i Google Cloud. Sejfy w chmurze publicznej mogą zapewniać elastyczność konfiguracji w celu spełnienia potrzeb klientów.[6, 7, 8]

Sejf Rubrik Cyber Recovery jest komponentem rozwiązania Rubrik Security Cloud. Sejf do odzyskiwania danych, udostępniany w modelu oprogramowania jako usługi, korzysta z pamięci masowej tylko na platformie Microsoft Azure. Wiele publicznie dostępnych dokumentów, które znaleźliśmy w ramach badania, wiąże sejf Rubrik Cyber Recovery z Rubrik Cloud Vault, warstwą kopii zapasowych, która zapewnia niezmienność.[9, 10] Taki sejf nie wymaga dodatkowego sprzętu i może być używany przez dowolną wersję platformy Rubrik Cloud Data Management (CDM), począwszy od wersji 6.02.

Niezmienność

Niezmienność oznacza stan trwałości lub niemożliwości zmiany. Niezmienne kopie zapasowe i ich kopie umożliwiają administratorom uzyskanie trwałych plików, których użytkownicy ani systemy nie mogą modyfikować ani usuwać, dopóki nie upłynie wyznaczony czas. Po tym czasie pliki „staczają się" — rozwiązanie automatycznie je usuwa. Rozwiązania zazwyczaj realizują ten proces za pomocą zasad lub definicji, które określają, jak system ma traktować pliki.[11]

Niezmienność w rozwiązaniu Dell PowerProtect Cyber Recovery opiera się na blokadach przechowywania za pośrednictwem funkcji Retention Lock, która zapobiega usunięciu lub modyfikacji (na pewien czas), bądź wymuszonemu wcześniejszemu wygaśnięciu kopii zapasowych. (Urządzenie PPDD ma system plików tylko do dołączania, niezależnie od tego, czy organizacja włączyła funkcję Retention Lock, czy nie[12]). Klienci firmy Dell zarządzają kopiami zapasowymi za pomocą partycji PPDD MTree, które są zdefiniowanymi przez użytkowników partycjami logicznymi z niezależnymi ustawieniami przechowywania, przypisywanymi przez nich jako miejsca docelowe aplikacji do tworzenia kopii zapasowych.[13] Klienci mają do wyboru dwa typy blokad przechowywania: oparte na ładzie korporacyjnym i zgodności. Blokady oparte na zgodności są opcją bardziej rygorystyczną i bezpieczniejszą. Klienci włączają blokady przechowywania dla poszczególnych partycji MTree, co oznacza, że wszystkie pliki w danej partycji MTree będą zgodne z definicją blokady przechowywania dla tej partycji MTree, oraz określają czas przechowywania poszczególnych plików. Gdy klienci zdefiniują blokadę przechowywania opartą na zgodności, żaden użytkownik ani system nie może jej usunąć. Administrator może cofnąć blokadę przechowywania opartą na ładzie korporacyjnym, co jest mniej rygorystyczną opcją.[14]

Niezmienność w rozwiązaniu firmy Rubrik opiera się również na blokadach przechowywania zapobiegających usunięciu lub wymuszonemu wcześniejszemu wygaśnięciu kopii zapasowych. Podobnie jak w przypadku rozwiązania PowerProtect Cyber Recovery, rozwiązanie Rubrik dołącza nowe dane do systemu plików, zamiast nadpisywać istniejące dane. Rozwiązanie tworzy odciski palców przychodzących danych i przechowuje je wraz z danymi. **Rozwiązanie Rubrik nie włącza domyślnie blokad przechowywania**, a klienci muszą wysyłać zgłoszenie do działu wsparcia firmy Rubrik lub włączyć regułę dwóch osób, aby zezwolić na blokady przechowywania. (Przed wprowadzeniem rozwiązania Rubrik Cloud Data Management w wersji 7.0.1 klienci musieli kontaktować się z działem wsparcia firmy Rubrik, aby włączyć blokady przechowywania. Dokumentacja firmy Rubrik nie określa jasno, czy klienci mogą nadal kontaktować się z działem wsparcia w tym celu). Po włączeniu przez klientów blokady przechowywania uniemożliwiają użytkownikom i systemom usuwanie danych o parametrach innych niż zdefiniowane. Blokady przechowywania w rozwiązaniu firmy Rubrik wymagają zewnętrznego serwera Network Time Protocol (NTP) do synchronizacji czasu, co może dawać cyberprzestępcom możliwość manipulowania wzorcowym źródłem NTP w taki sposób, aby blokady przechowywania przedwcześnie wygasały.[15]

> *„Rozwiązanie Rubrik nie włącza domyślnie blokad przechowywania, a klienci muszą wysyłać zgłoszenie do działu wsparcia firmy Rubrik lub włączyć regułę dwóch osób, aby zezwolić na blokady przechowywania."*

Licencjonowanie i subskrypcje

Dell PowerProtect Cyber Recovery to rozwiązanie licencjonowane. Podczas instalacji firma Dell domyślnie instaluje 90-dniową licencję próbną. Po upływie 90 dni klienci muszą zakupić nową licencję, aby nadal korzystać z produktu. Firma Dell oferuje zarówno licencje standardowe (stałe), jak i oparte na subskrypcji.

Firma Rubrik integruje Rubrik Cyber Recovery z rozwiązaniem Rubrik Security Cloud (RSC). Klienci muszą mieć subskrypcję Rubrik Enterprise Edition, aby korzystać z systemu Rubrik Cyber Recovery. Okres subskrypcji wynosi trzy lata.[16, 17] W przypadku awarii RSC obciążenia robocze SAP HANA i Db2 wymagają narzędzi innych firm do odzyskania danych, co może wiązać się z dodatkowymi kosztami subskrypcji.[18]

Dostęp administracyjny

Zarządzanie systemem Dell PowerProtect Cyber Recovery odbywa się lokalnie w zależności od topologii wybranej przez klientów do wdrożenia. Ponieważ to rozwiązanie inicjuje odzyskiwanie z sejfu, administratorzy logują się do interfejsu użytkownika zarządzania z dowolnego miejsca, w którym znajduje się ich sejf. Sejfy lokalne oferują administratorom dostęp lokalny bez konieczności dostępu do Internetu, który cyberataki mogą poważnie naruszyć, np. ataki typu „odmowa usługi",

lub zabezpieczenie danych przez zerwanie połączenia z Internetem, zgodnie z zaleceniami National Institute of Standards and Technology (NIST). Sejfy w kolokacjach umożliwiają fizyczny dostęp do urządzenia z lokalizacji zdalnej i korzystanie z połączeń poza publicznym Internetem. Sejfy oparte na chmurze wymagają dostępu do Internetu w celu odzyskania danych, co mogłoby opóźnić odzyskanie lokalne do czasu zakończenia cyberataku i wznowienia normalnej łączności sieciowej.

Zarządzanie rozwiązaniem Rubrik Cyber Recovery wymaga dostępu do usługi Rubrik Security Cloud, a zatem dostępu do Internetu. Jak już zauważyliśmy, ten rodzaj łączności może opóźnić lokalne odzyskanie danych do czasu, gdy funkcjonalność sieci powróci do normy po cyberataku.

Ponieważ klienci muszą mieć dostęp do usługi RSC, aby korzystać z funkcji rozwiązania Rubrik Cyber Recovery, usługa RSC staje się pojedynczym miejscem awarii. Gdyby ta usługa stała się niedostępna dla klienta, utrudniłoby mu to odzyskanie danych z sejfu. Firma Rubrik może odzyskać 10 obciążeń roboczych podczas przerwy w działaniu usługi RSC, ale odzyskanie dwóch bazodanowych obciążeń roboczych wymaga narzędzi innych firm i pomocy działu wsparcia firmy Rubrik.[19, 20] Ponadto zhakowane konta administratorów lub cyberprzestępcy z dostępem do platformy RSC zyskują wówczas dostęp do wszystkich zasobów, a nie jedynie pojedynczego sejfu.

Uzyskaj dodatkową pomoc dzięki usłudze Managed Detection and Response firmy Dell

Niektóre organizacje mogą nie czuć się pewnie w samodzielnym zarządzaniu cyberbezpieczeństwem. Firma Dell oferuje tym klientom w pełni zarządzaną usługę Managed Detection and Response (MDR), która polega na monitorowaniu i wykrywaniu zagrożeń i czynników ryzyka, a także współpracy z klientami w ograniczaniu ryzyka. Według firmy Dell usługa obejmuje następujące elementy:[21]

- Zaufana pomoc techniczna, w tym porady ekspertów dotyczące wdrażania i konfigurowania obsługiwanych przez firmę Dell platform analizy zabezpieczeń z rozszerzonym wykrywaniem zagrożeń i reagowaniem na nie (XDR)
- Reagowanie na zagrożenia i konfiguracja zabezpieczeń, w tym maksymalnie 40 godzin konfiguracji zabezpieczeń związanych z usługą na kwartał
- Wykrywanie i badanie zagrożeń przez 24 godziny na dobę, 7 dni w tygodniu, w tym proaktywne wyszukiwanie zagrożeń specyficznych dla środowiska każdego klienta w celu wykrycia nowych zagrożeń lub wariantów znanych zagrożeń, które omijają systemy zabezpieczeń
- Inicjowanie reagowania na incydenty związane z cyberbezpieczeństwem, w tym 40 godzin rocznie zdalnej pomocy w reagowaniu na incydenty, która umożliwia szybkie rozpoczęcie działań dochodzeniowych

W połączeniu z usługami APEX Cyber Recovery Services usługa MDR umożliwia klientom wybór spośród wielu opcji monitorowania, wykrywania i ograniczania zagrożeń i czynników ryzyka. Dostępność opcji może przekładać się na rozszerzoną ochronę lub podejście hybrydowe, które odpowiada potrzebom Twojej organizacji.

Więcej informacji na temat usługi MDR można znaleźć na stronie **https://www.dell.com/en-us/dt/services/managed-services/managed-workplace-services/managed-detection-response.htm**.

Bezproblemowość

Konfiguracja

Konfiguracja Dell PowerProtect Cyber Recovery obejmuje instalację oprogramowania w systemie Linux lub utworzenie urządzenia VMware® vSphere® na podstawie szablonu Open Virtualization Format (OVF). Instalacja oprogramowania wymaga 14 kroków,[22] podczas gdy alternatywne wdrożenie urządzenia vSphere wymaga 8 kroków i zajmuje 5 minut.[23] Po instalacji administratorzy mogą uzyskać dostęp do rozwiązania za pośrednictwem przeglądarek internetowych z poziomu izolowanego środowiska.

Klienci muszą oddzielnie wdrożyć CyberSense, czyli w pełni zautomatyzowany i zintegrowany inteligentny silnik analizy zabezpieczeń.[24] Instrukcje instalowania silnika CyberSense w rozwiązaniu Dell PowerProtect Cyber Recovery nie są publicznie dostępne.[25]

Firma Dell oferuje wiele wskaźników, które użytkownicy mogą dostosować, w tym cel wykrywania zniszczeń (DDO), cel oceny zniszczeń (DAO), punkt Cyber Recovery (CRP), czas Cyber Recovery (CRT), interwał synchronizacji Cyber Recovery oraz liczbę kopii danych Cyber Recovery. Firma Dell zaleca również scharakteryzowanie danych, które wymagają ochrony. Takie dane mogą być krytyczne dla misji, krytyczne dla działalności biznesowej, zależne od podstawowych usług infrastruktury lub innych aplikacji lub ogólne, takie jak pliki binarne aplikacji, obrazy rozruchowe i katalogi kopii zapasowych. Szeroka gama opcji daje klientom pełną kontrolę nad środowiskiem kopii zapasowych oraz możliwość dostosowania klasyfikacji danych. Dział Dell Consulting Services może również udzielić dalszej pomocy i przekazać sugestie.[26]

Konfiguracja rozwiązania firmy Rubrik również obejmuje wiele kroków. Przed utworzeniem klastra dział wsparcia firmy Rubrik musi zainstalować i skonfigurować oprogramowanie Rubrik CDM. Wówczas administrator pobiera i instaluje najnowszą lub żądaną wersję CDM (15 kroków).[27] Następnie administrator może skonfigurować klaster Rubrik przy użyciu interfejsu użytkownika lub interfejsu wiersza polecenia. Klaster można skonfigurować za pomocą interfejsu użytkownika lub interfejsu wiersza polecenia, przy czym oba podejścia wymagają 24 kroków.[28, 29] Potem administrator może zarejestrować klastry Rubrik za pomocą metody online (12 kroków)[30] lub offline (18 kroków).[31] Następnie administrator włącza uwierzytelnianie wieloskładnikowe (MFA), co wymaga 13 kroków.[32] Na koniec administrator dodaje konto początkowe (6 kroków) i wszelkie pozostałe konta.[33] Rysunek 3 przedstawia maksymalną liczbę możliwych kroków przy konfigurowaniu każdego rozwiązania Cyber Recovery.

Klienci firmy Rubrik nie mogą dostosowywać innych wskaźników, co może zmniejszać elastyczność spełniania potrzeb. Jeden z recenzentów stwierdził: „Większa część interfejsu użytkownika jest dość prosta i łatwa, ale w niektórych miejscach brakuje opisu, do czego służy dana opcja, albo brakuje opcji. Wprawdzie obsługa jest łatwa dla użytkownika, ale brakuje wielu opcji dostosowywania, co wymaga otwarcia tunelu wsparcia, aby osoba z działu wsparcia mogła wprowadzić zmiany w środowisku klienta”.[34]

Rysunek 3. Maksymalna liczba możliwych kroków przy konfigurowaniu rozwiązań Dell PowerProtect Cyber Recovery i Rubrik Security Cloud. Im mniej, tym lepiej. Źródło: Principled Technologies.

ryzykiem

Zaobserwowaliśmy, że po skonfigurowaniu interfejsy użytkownika do wykonywania codziennych czynności konserwacyjnych są podobne w przypadku rozwiązań firm Dell i Rubrik. Po konfiguracji klienci mogą skonfigurować rozwiązanie Dell PowerProtect Cyber Recovery do wykonywania następujących zadań:[35, 36]

- Automatyczne generowanie raportów z zadań Cyber Recovery zgodnie z harmonogramem i w odpowiedzi na ręczne żądanie użytkownika
  - Użytkownik lub harmonogram tworzy zadanie, gdy inicjuje zasadę, operację odzyskiwania, wykonywanie kopii zapasowej systemu lub operację czyszczenia
- Automatyczne monitorowanie stanu sejfu, pojemności pamięci masowej, operacji Cyber Recovery, alertów w przypadku niepowodzenia kopiowania/synchronizacji lub awarii sejfu Cyber Recovery oraz zadań Cyber Recovery
- Automatyczne i ciągłe skanowanie w poszukiwaniu ataków, a następnie wyświetlanie alertów CyberSense, w kolejności ważności, z podaniem liczby plików, hostów, odnośnych zasad, wykrytych konkretnych zagrożeń, momentu czasowego ataku, aby można było znaleźć czystą kopię zapasową oraz listy uszkodzonych plików do wykorzystania w analizie ataku

Analogicznie, klienci mogą skonfigurować rozwiązanie Rubrik do wykonywania następujących zadań:[37]

- Automatyczne korzystanie z usługi Rubrik Security Cloud do śledzenia, monitorowania i wyświetlania wszystkich zdarzeń we wszystkich połączonych klastrach Rubrik. Usługa udostępnia trzy typy zdarzeń:[38]
  - Krytyczne — zdarzenia wymagające uwagi, takie jak niepowodzenie tworzenia kopii zapasowej, archiwizacji lub replikacji
  - Ostrzegawcze — ukończenie tworzenia kopii zapasowej, archiwizacji lub odzyskiwani
  - Informacyjne — tylko dla informacji
- Automatyczne i ciągłe skanowanie migawek w poszukiwaniu nowych i istniejących wskaźników naruszenia bezpieczeństwa za pomocą narzędzia Threat Monitor, które podaje czas ostatniego wykonania migawki przez rozwiązanie, oś czasu zdarzeń, czas wykrycia, liczbę zmienionych plików, liczbę podejrzanych plików, nazwę klastra oraz typ i nazwę obiektu

Obsługa obciążeń roboczych przy wykrywaniu anomalii

Zarówno Rubrik Security Cloud Data Threat Analytics, jak i CyberSense skanują wiele typów obciążeń roboczych, ale według źródeł, do których dotarliśmy, CyberSense obsługuje dwa razy więcej obciążeń roboczych przy wykrywaniu anomalii. Obejmuje to skanowanie następujących typów obciążeń roboczych:

- Maszyny wirtualne
- Podstawowa infrastruktura
- Pliki użytkownika, które mogą zawierać dokumenty, umowy i własność intelektualną
- Bazy danych
- Kopie zapasowe wykonane przez innych klientów

"Jeśli policzymy obsługiwane obciążenia robocze, które znaleźliśmy w publicznie dostępnych danych, okaże się, że CyberSense obsługuje 21 obciążeń roboczych przy wykrywaniu anomalii, podczas gdy rozwiązanie firmy Rubrik obsługuje ich 7."

Jeśli policzymy obsługiwane obciążenia robocze, które znaleźliśmy w publicznie dostępnych danych, okaże się, że CyberSense obsługuje 21 obciążeń roboczych przy wykrywaniu anomalii, podczas gdy rozwiązanie firmy Rubrik obsługuje ich 7. W związku z tym, zgodnie z publicznie dostępnymi danymi każdej firmy, CyberSense obsługuje dwa razy więcej obciążeń roboczych niż Rubrik Security Cloud Data Threat Analytics. Im więcej danych może przeskanować rozwiązanie Cyber Recovery, tym większa szansa na znalezienie złośliwego oprogramowania lub innego zagrożenia.

Obsługa obciążeń roboczych maszyn wirtualnych

Obciążenia maszyn wirtualnych to aplikacje, usługi lub zadania, które maszyny wirtualne uruchamiają na fizycznym serwerze hosta lub w środowisku chmurowym. Ponieważ te obciążenia robocze mogą różnić się funkcjami i wieloma innymi cechami, które mogą zwiększyć ich narażenie na złośliwe oprogramowanie, skanowanie maszyn wirtualnych ma kluczowe znaczenie. Rozwiązanie Rubrik Security Cloud Data Threat Analytics, które „obejmuje wykrywanie anomalii, monitorowanie zagrożeń, wyszukiwanie zagrożeń i usługi odzyskiwania danych chronionego zasobu”[39], obsługuje skanowanie następujących obciążeń roboczych maszyn wirtualnych:[40]

- VMware
- Nutanix® AHV
- Microsoft Hyper-V
- Microsoft Azure

CyberSense obsługuje skanowanie następujących obciążeń roboczych maszyn wirtualnych:[41, 42, 43]

- VMware
- Amazon Web Services (AWS)
- Hyper-V z kopiami zapasowymi Dell Avamar lub Dell NetWorker

Firma VMware twierdzi, że „aż 80% wirtualizowanych obciążeń roboczych działa w technologii VMware”.[44] W pierwszym kwartale 2024 r. najpopularniejszy dostawca na rynku usług infrastruktury chmurowej, czyli Amazon Web Services (AWS), kontrolował 31% całego rynku. Na drugim miejscu znajduje się Microsoft Azure z 25-procentowym udziałem w rynku.[45]

Podstawowa infrastruktura

Podstawowa infrastruktura obejmuje podstawowe komponenty i usługi, które umożliwiają działanie środowiska technologicznego. Wykrywanie złośliwego oprogramowania na tym poziomie może pomóc w zmniejszeniu wagi ataku, ponieważ podstawowe funkcje infrastruktury mogą mieć wpływ na wiele systemów i użytkowników. Dokumentacja rozwiązania Rubrik Security Cloud nie wspomina o obsłudze skanowania żadnej podstawowej infrastruktury.[46]

Z kolei CyberSense obsługuje skanowanie następującej infrastruktury podstawowej:[47]

- Active Directory
- DNS
- LDAP

Pliki użytkownika, które mogą zawierać dokumenty, umowy i własność intelektualną

Rubrik Security Cloud Data Threat Analytics obsługuje skanowanie następujących plików użytkowników:[48]

- Zestawy plików i zestawy danych NAS
- Grupy woluminów systemu Windows
- Linux i Windows

CyberSense może skanować pliki użytkowników systemów Linux i Windows.[49]

Skanowanie baz danych

CyberSense skanuje 7, a RSC Data Threat Analytics 0

Bazy danych

Aplikacje mogą korzystać z różnych typów baz danych do różnych celów, więc możliwość wykrycia obecności złośliwego oprogramowania w różnych bazach danych może mieć kluczowe znaczenie dla szybkiej reakcji. Rubrik Security Cloud Data Threat Analytics może tworzyć kopie zapasowe baz danych, ale nie znaleźliśmy publicznej dokumentacji, w której wspomniano, że może skanować kopie zapasowe tych baz danych.

CyberSense obsługuje skanowanie następujących baz danych na poziomie strony:[50]

- SQL
- Oracle®
- SAP HANA
- Db2
- PostgreSQL
- Epic® Caché
- MariaDB/MySQL

Kopie zapasowe wykonane przez innych klientów

Niektóre organizacje mogą mieć kopie zapasowe danych z baz danych wielu dostawców, aby zapewnić nadmiarowość, zachować zgodność z przepisami lub z innego ważnego powodu. Dokumentacja rozwiązania Rubrik Security Cloud nie wspomina o obsłudze skanowania kopii zapasowych wykonanych przez innych klientów tworzenia kopii zapasowych.[51]

Wyraźną przewagę w tej kategorii ma silnik CyberSense, który obsługuje skanowanie kopii zapasowych wykonanych przez następujących klientów tworzenia kopii zapasowych:[52, 53, 54]

- DNAS
- Exchange
- SQL
- Avamar
- NetWorker
- Commvault
- Veritas NetBackup

Technologia skanowania

Rubrik Security Cloud zawiera wiele narzędzi do skanowania i do pomocy w skanowaniu w Data Threat Analytics:

- Oprogramowanie Rubrik Anomaly Detection wyświetla podejrzane pliki, zmiany w migawkach,[55] i szczegóły anomalii jako zdarzenia anomalii, które klienci mogą badać i używać w badaniu migawek.[56] Oprogramowanie udostępnia również opcje odzyskiwania.[57]
- Oprogramowanie Rubrik VM Encryption Detection wykrywa ataki na pliki dysków wirtualnych VMware vSphere.[58]
- Oprogramowanie Rubrik Threat Monitoring wyświetla informacje o wykrytych zagrożeniach i dopasowaniach.[59]
- Funkcja Rubrik Threat Hunt to inicjowane przez użytkownika skanowanie w poszukiwaniu oznak naruszenia bezpieczeństwa.[60]
- Funkcja Rubrik Quarantine izoluje obiekty wykryte przez funkcję Threat Hunt.[61]

Rozwiązanie Rubrik RSC zawiera również łączniki usługi Rubrik Backup Service dla każdego klastra Rubrik.

Klienci firmy Rubrik muszą wybrać odpowiednie narzędzie do danego zadania, mogą być zmuszeni do ręcznego zainicjowania skanowania lub użycia wielu narzędzi, aby wykonać zadanie. Z kolei firma Dell oferuje jedną opcję skanowania CyberSense, co może ułatwiać klientom zarządzanie i administrowanie.

Skanowanie CyberSense sięga głębiej niż jedynie „skanowanie powierzchowne", jak w przypadku Rubrik RSC Data Threat Analytics. CyberSense wykonuje pełne skanowanie zawartości plików i skanowanie baz danych na poziomie strony oraz może wykryć częściowe szyfrowanie plików.[62] Narzędzie wykorzystuje bazę danych uczenia maszynowego (ML) wytrenowaną przez Index Engines na tysiącach zagrożeń dla danych i zawiera ponad 200 punktów analitycznych do wykrywania uszkodzeń danych.[63] W przeciwieństwie do Rubrik Threat Monitoring i Threat Hunt, CyberSense nie polega na zewnętrznych agencjach Threat Intelligence do uzyskiwania sygnatur złośliwego oprogramowania. Zamiast tego odkrywa nowe zagrożenia.[64]

CyberSense nie polega również na arbitralnych progach akceptowalnych zmian w plikach lub poziomach entropii między migawkami, które mogą prowadzić do wyników fałszywie ujemnych. Ponadto nie trenuje swojej bazy danych uczenia maszynowego na podstawie poprzednich zachowań klientów jako punktu odniesienia.[65, 66, 67]

„CyberSense nie polega również na arbitralnych progach akceptowalnych zmian w plikach lub poziomach entropii między migawkami, które mogą prowadzić do wyników fałszywie ujemnych…."

Oprogramowanie firmy Rubrik do wykrywania anomalii polega wyłącznie na metadanych przy ustalaniu, czy migawka jest uszkodzona, przed wykonaniem jakiejkolwiek analizy zawartości. W przeciwieństwie do uczenia maszynowego na bieżąco w przypadku silnika CyberSense, oprogramowanie Rubrik wykrywa uszkodzenie dopiero po uzyskaniu sygnatur. Wykrywanie anomalii w rozwiązaniu firmy Rubrik wymaga zbudowania modelu behawioralnego w celu zdefiniowania normalnego zachowania klienta jako punktu odniesienia. Jego ustalenie może wymagać

utworzenia kilku kopii zapasowych. Model behawioralny firmy Rubrik wymaga co najmniej dwóch kopii zapasowych, aby utworzyć punkt odniesienia dla typowych zmian w systemie plików, gdy nie ma żadnych ataków. Jednak pojedynczy zestaw statystyk zmian może nie wystarczyć do ustalenia, co jest typowe. Zdarzenia biznesowe mogą wywoływać większą lub mniejszą aktywność lub więcej podejrzanych typów aktywności, które nie wystąpiły między pierwszą a drugą migawką w rozwiązaniu Rubrik. Im więcej kopii zapasowych analizuje rozwiązanie firmy Rubrik, tym dokładniej może wytrenować swój model behawioralny względem punktu odniesienia.[68, 69]

CyberSense przechowuje wszystkie swoje dane analityczne w sejfie. W potoku analizy zachowania systemu plików rozwiązanie Rubrik wysyła metadane o zmianach w systemie plików klienta do chmurowej platformy Polaris w celu przeprowadzenia analizy zachowania, otwierając możliwość ataku.[70]

Klienci mogą korzystać z narzędzi Rubrik Threat Monitoring i Threat Hunt tylko w wersji Rubrik Enterprise.[71] Klienci muszą przeprowadzać skanowanie Threat Hunt z uprawnieniami kontroli dostępu opartej na rolach (RBAC), a użytkownicy muszą wskazać, których konkretnie oznak naruszenia bezpieczeństwa (IOC) chcą szukać.[72] Nie jest to najlepsza praktyka branżowa.[73] Podobnie jak CyberSense, Threat Hunt obsługuje zestawy plików VMware, AHV, Hyper-V i NAS oraz serwery Linux i Windows.[74]

Poniższe sekcje zawierają bardziej szczegółowe informacje na temat sposobu wykrywania zagrożeń przez rozwiązanie firmy Rubrik.

Metadane i statystyki systemu plików

Model behawioralny uczenia maszynowego wykrywania anomalii w rozwiązaniu firmy Rubrik rejestruje zmiany w systemie plików od ostatniej migawki — takie jak liczba dodanych, usuniętych lub przeniesionych plików — jako metadane.[75] Następnie model uczenia maszynowego trenuje się na tych zmianach, aby utworzyć „punkt odniesienia" modelu behawioralnego dla systemu plików. Rozwiązanie firmy Rubrik oznacza migawkę jako anomalię, jeśli wykryje zbyt wiele zmian. Po oznaczeniu migawki przez analizę zachowania rozwiązanie rozpoczyna analizę zawartości plików.[76] Monitorowanie metadanych może stanowić dodatkową warstwę zabezpieczeń, ale może nie zapewniać niezbędnej ochrony, która pomaga eliminować lub ograniczać przestoje spowodowane zdarzeniami.

> *„CyberSense nie potrzebuje punktu odniesienia; monitoruje i analizuje zmiany zawartości plików i baz danych względem pierwszych kopii zapasowych."*

Z drugiej strony, **silnik CyberSense nie potrzebuje punktu odniesienia; monitoruje i analizuje zmiany zawartości plików i baz danych względem pierwszych kopii zapasowych.** Podejście CyberSense oferuje większą szczegółowość, ponieważ oprogramowanie analizuje nawet fragmenty pliku lub poszczególne strony bazy danych. Podobnie jak w przypadku rozwiązania firmy Rubrik, skanowanie w oprogramowaniu CyberSense obejmuje właściwości metadanych i przekazuje wyniki do silnika ML. W przeciwieństwie do rozwiązania firmy Rubrik, CyberSense nie ogranicza się do skanowania metadanych, a firma Index Engines wytrenowała swój silnik ML na atakach udokumentowanych przez firmę Index Engines, a nie na sygnaturach czy wcześniejszych zachowaniach klientów.[77, 78]

Progi

Podczas analizy zachowania system ML firmy Rubrik określa, jakie jest prawdopodobieństwo, że w systemie plików wystąpiła anomalia. Jeśli rozwiązanie firmy Rubrik uzna to za prawdopodobne, przeprowadzi analizę zawartości. Może to bazować na progu „nietypowego zachowania" wyznaczonym przez model behawioralny. Na przykład rozwiązanie Rubrik może oznaczać nietypowe zachowanie, gdy stwierdzi wiele nowych lub zmodyfikowanych plików, albo zwiększoną losowość lub wskaźniki szyfrowania.[79] Podczas analizy zawartości oprogramowanie Rubrik Anomaly Detection wyświetla zmiany w zawartości plików i oblicza prawdopodobieństwo szyfrowania przez obliczenie entropii systemu plików. Entropia systemu plików pomaga wykazać prawdopodobieństwo, że atak ransomware zaszyfrował pliki. Jeśli entropia przekroczy próg anomalii, rozwiązanie ostrzeże użytkownika.[80, 81] Skuteczność wykrywania uszkodzenia danych zależy od rygorystyczności progu. Zbyt duża swoboda może powodować wyniki fałszywie ujemne, a tym samym dawać fałszywe poczucie bezpieczeństwa.[82] Klienci muszą odpowiednio ustawić progi.

Z kolei silnik CyberSense sprawdza pliki pod kątem częściowego zaszyfrowania, skanując ich zawartość i wykrywając uszkodzenie danych z poziomem ufności 99,99% (według firm Dell i Index Engines).[83]

Sygnatury i rozszerzenia plików

Narzędzia Rubrik Threat Monitoring i Threat Hunt skanują migawki w poszukiwaniu oznak naruszenia bezpieczeństwa (IOC). Gdy jedno z wielu źródeł Threat Intelligence monitorowanych przez firmę Rubrik odkryje nową IOC, narzędzie Threat Monitoring przesyła informację o zagrożeniu zawierającą reguły Yet Another Ridiculous Acronym (YARA) służące do identyfikacji nowego złośliwego oprogramowania, znane również jako sygnatura złośliwego oprogramowania, do wszystkich klastrów rozwiązania firmy Rubrik. Następnie klastry rozpoczną skanowanie.[84] Niedawny raport WatchGuard sugeruje, że 57,8% złośliwego oprogramowania unika wykrywania sygnatur. Zaawansowane złośliwe oprogramowanie, takie jak BianLian, może wykorzystywać metody unikania rozpoznawania sygnatur, a nowe warianty złośliwego oprogramowania mogą mieć nieco inne sygnatury niż oryginalne. W związku z tym Threat Intelligence może utrudniać wykrywanie najnowszych zagrożeń.[85]

Dla porównania, CyberSense korzysta z ponad 200 narzędzi analitycznych i udostępnia model uczenia maszynowego wytrenowany na tysiącach wariantów oprogramowania ransomware. Firma Index Engines wykazała, że metoda stosowana przez CyberSense może wykrywać wcześniej nieznane, wyrafinowane warianty bez pobierania sygnatur,[86] co jest kolejną zaletą niewymagającą korzystania z Internetu w czasie wystąpienia zdarzenia.

Zdarzenia masowego szyfrowania

Rozwiązanie firmy Rubrik monitoruje system pod kątem zdarzeń masowego szyfrowania, obliczając entropię całego systemu plików.[87] Oprogramowanie CyberSense jest znacznie bardziej wnikliwe. Nie tylko skanuje cały system plików czy nawet każdy pojedynczy plik, ale wręcz fragmenty wewnętrznej zawartości plików. Według Index Engines, obliczanie entropii jedynie całego pliku, a nie jego fragmentów, „wykryje tylko ekstremalne szyfrowanie całego pliku" lub zdarzenia masowego szyfrowania.[88]

Możliwość odtworzenia

Na podstawie dokumentacji uważamy, że odtwarzanie systemów czy odzyskiwanie danych za pomocą rozwiązania Dell PowerProtect Cyber Recovery jest prostszym i sprawniejszym procesem niż w przypadku rozwiązania firmy Rubrik. W tej sekcji raportu, w tym jej podsekcjach, porównaliśmy funkcje odzyskiwania dostępne w obu rozwiązaniach oraz sposób implementacji takich funkcji w tych rozwiązaniach.

Dokumentacja firmy Rubrik zawiera informacje o tym, które z jej funkcji odzyskiwania działają na poszczególne typy maszyn wirtualnych. Może się wydawać, że stanowi to przydatny poziom szczegółowości, jednak wiele zastrzeżeń i wariantów sprawia, że odzyskiwanie jest skomplikowane. Na przykład, gdy klienci firmy Rubrik chcą odzyskać dane, pliki i systemy, muszą wybrać obiekty migawek, które chcą uwzględnić w swoim planie odzyskiwania. Po utworzeniu jednego lub większej liczby planów odzyskiwania firma Rubrik oferuje wiele opcji odzyskiwania, w tym następujące:[89, 90, 91, 92, 93]

- Odzyskiwanie plików przez pobieranie lub nadpisywanie i odtwarzanie do osobnego folderu, eksport do innego hosta lub eksport do usługi klastrowanej
- Odzyskiwanie plików maszyn wirtualnych przez pobieranie lub nadpisywanie i odtwarzanie do osobnego folderu lub eksport do innej maszyny wirtualnej
- Pełne odzyskiwanie migawki maszyny wirtualnej lub dysku za pomocą następujących opcji:
  - Live Mount, czyli utworzenie nowej maszyny wirtualnej na podstawie migawki
  - Montowanie dysków wirtualnych, które powoduje utworzenie nowych dysków wirtualnych na podstawie migawki
  - Instant Recovery, czyli zastąpienie bieżącej maszyny wirtualnej nową maszyną wirtualną utworzoną przez migawkę
  - Export, czyli utworzenie nowej maszyny wirtualnej na podstawie migawki w wybranym magazynie danych
  - Odzyskiwanie wsadowe maszyn wirtualnych
- Masowe odzyskiwanie Cyber Recovery za pomocą opcji Live Mount i Export
- Funkcja Rubrik Security Cloud Orchestrated Application Recovery do odtwarzania maszyn wirtualnych po awarii do izolowanej piaskownicy, lokalizacji zdalnej lub lokalnej

Odzyskiwanie wsadowe firmy Rubrik wykazuje dodatkową złożoność. W tabeli 1 przedstawiono funkcje odzyskiwania wsadowego udostępniane przez firmę Rubrik w zależności od monitora maszyny wirtualnej.[94]

Tabela 1. Funkcje odzyskiwania wsadowego udostępniane przez firmę Rubrik dla różnych monitorów maszyn wirtualnych. Źródło: Rubrik.

Opcje tworzenia maszyn wirtualnych				
	Live Mount	**Live Mount z opcjonalną migracją**	**Eksport**	**Instant Recovery**
Maszyny wirtualne vSphere	Dostępne, z użyciem klastra Rubrik jako magazynu danych	Niedostępna	Dostępne, z użyciem magazynu danych odzyskanego monitora maszyny wirtualnej	Dostępne, z użyciem klastra Rubrik jako magazynu danych
Maszyny wirtualne AHV	Dostępne, z użyciem klastra Rubrik jako magazynu danych	Dostępne, z użyciem klastra Rubrik jako magazynu danych i kontenera Nutanix do wszystkich kolejnych zapisów	Dostępne, z użyciem kontenera Nutanix jako magazynu danych	Niedostępna
Maszyny wirtualne Hyper-V	Dostępne, z użyciem klastra Rubrik jako magazynu danych	Niedostępna	Dostępne, z użyciem magazynu danych odzyskanego monitora maszyny wirtualnej	Dostępne, z zastąpieniem bieżącej maszyny wirtualnej nową maszyną wirtualną z migawki. Używa klastra Rubrik jako magazynu danych.

W przypadku rozwiązania Rubrik odzyskany magazyn danych zwykle znajduje się w klastrze Rubrik, a nie w środowisku produkcyjnym, co może powodować problemy. Problemy te przedstawiamy w następnej sekcji, "Rubrik limitations". Z kolei funkcja PowerProtect może umieszczać odzyskane dane w środowiskach odzyskiwania lub produkcyjnych, aby zapewnić szybsze i płynniejsze odzyskiwanie, które może zminimalizować przestoje.

Tabela 2 zawiera dodatkowe informacje od firmy Rubrik na temat odzyskiwania maszyn wirtualnych vSphere.[95] Jak pokazano w tabeli, większość magazynów danych odzyskiwania vSphere znajduje się w klastrze Rubrik.

Tabela 2. Funkcje odzyskiwania udostępniane przez rozwiązanie firmy Rubrik dla maszyn wirtualnych vSphere. Źródło: Rubrik.

Funkcje odzyskiwania udostępniane przez rozwiązanie firmy Rubrik dla maszyn wirtualnych vSphere				
Czynność	**Magazyn danych**	**Stan zasilania**	**Sieć**	**Źródłowa macierz VM**
Odzyskiwanie plików	Nie dotyczy	Nie dotyczy	Nie dotyczy	Bez wpływu
Live Mount	Lokalny klaster Rubrik	Wł. lub wył.	Rozłączono	Bez wpływu
Montowanie dysków wirtualnych	Lokalny klaster Rubrik	Wł.	Rozłączono	Bez wpływu
Instant Recovery	Lokalny klaster Rubrik	Wł.	Połączenie (opcjonalne)	Wyłączenie zasilania i zmiana nazwy
Eksport	Magazyn danych monitora maszyny wirtualnej	Wyłączony	Rozłączono	Bez wpływu
Odzyskiwanie na miejscu	Magazyn danych monitora maszyny wirtualnej	Wł.	Tak samo jak w przypadku źródłowej maszyny wirtualnej	Odzyskiwanie na miejscu zastępuje pliki dysku wirtualnego źródłowej maszyny wirtualnej danymi dysku wirtualnego z migawki, bez zmiany właściwości maszyny wirtualnej

Rozwiązanie firmy Rubrik nie implementuje szeroko zakrojonego odzyskiwania zbiorczego, a opcje odzyskiwania zbiorczego są ograniczone i złożone. Jak dokładniej wyjaśniono w sekcji "Dell PowerProtect Data Manager offers the equivalent of Rubrik "mass restore"" tego raportu, funkcja Dell PowerProtect działa sprawnie i jest prostsza.

Wyjaśnienie nieporozumień dotyczących odzyskiwania masowego

Firma Rubrik reklamuje odzyskiwanie masowe jako szybkie przywracanie działalności biznesowej poprzez odzyskiwanie danych aplikacji, plików lub użytkowników na dużą skalę.[96] Oferuje wiele opcji odzyskiwania zbiorczego. Jednak rozwiązanie firmy Rubrik zwykle przechowuje odzyskane dane w klastrze Rubrik, a nie w środowisku produkcyjnym.[97] Obciążenia robocze wymagają dostępności systemu firmy Rubrik do momentu ukończenia migracji przez rozwiązanie. Lokalny klaster firmy Rubrik jest pamięcią masową warstwy 3, więc klienci muszą przeprowadzić dodatkową migrację do swojego środowiska produkcyjnego, aby powrócić do planowanych poziomów wydajności. Ze względu na to pojedyncze miejsce awarii i zmniejszoną wydajność do czasu zakończenia migracji przez system nie możemy uznać odzyskiwania za zakończone, dopóki rozwiązanie firmy Rubrik nie przywróci obciążeń roboczych do środowiska produkcyjnego.

Oprogramowanie Dell PowerProtect również oferuje odzyskiwanie zbiorcze, umożliwiając użytkownikom wybranie wielu maszyn wirtualnych do odzyskania w interfejsie użytkownika odzyskiwania.

Program Dell PowerProtect Data Manager oferuje odpowiednik funkcji „odzyskiwania masowego" oferowanej przez firmę Rubrik

W porównaniu z rozwiązaniem firmy Rubrik rozwiązanie firmy Dell również oferuje wiele równoważnych opcji odzyskiwania dla maszyn wirtualnych vSphere. Dell PowerProtect może umieszczać dane maszyn wirtualnych w środowiskach odzyskiwania lub produkcyjnych. Większość opcji firmy Rubrik umieszcza dane tylko w klastrze Rubrik. W tabeli 3 przedstawiono opcje odzyskiwania danych w rozwiązaniu firmy Dell.[98, 99, 100, 101]

Tabela 3. Opcje odzyskiwania danych w rozwiązaniu firmy Dell. Źródło: Principled Technologies.

Opcje odzyskiwania danych w rozwiązaniu firmy Dell	
Typ	**Informacje o funkcji**
Przywracanie na poziomie plików	Przywraca tylko zainfekowane pliki na miejscu lub przez cofnięcie
Przywracanie maszyny wirtualnej na żywo	Przywraca maszynę wirtualną do klastra z późniejszą migracją do środowiska produkcyjnego
Przywracanie do nowego środowiska	Przywraca do oryginalnego lub nowego środowiska (np. pomieszczenia czystego lub infrastruktury odzyskiwania), a w trakcie przywracania użytkownicy mogą wybrać wiele maszyn wirtualnych jednocześnie do przywrócenia zbiorczego lub na dużą skalę
Dostęp/ przywracanie maszyny wirtualnej na żywo	Tworzy izolowaną kopię danych produkcyjnych
Aranżacja odzyskiwania	Umożliwia administratorom planowanie odzyskiwania lub udostępnianie go na żądanie; nadaje priorytet automatycznemu odzyskiwaniu maszyn wirtualnych do środowiska produkcyjnego lub środowiska odzyskiwania

Ograniczenia rozwiązania firmy Rubrik

Rozwiązanie firmy Rubrik poddaje kwarantannie migawki zainfekowane złośliwym oprogramowaniem na potrzeby przyszłej analizy. Jednak rozwiązanie firmy Rubrik nie poddaje migawek kwarantannie domyślnie. Klienci mogą następnie pobrać pliki poddane kwarantannie i przeprowadzić ich analizę pod kątem zagrożeń samodzielnie lub za pomocą narzędzi innych firm, potencjalnie narażając się na infekcję złośliwym oprogramowaniem.[102, 103]

> *CyberSense przeprowadza swoją analizę bez konieczności wykonywania przez użytkownika własnych badań pod kątem zagrożeń, a ponadto automatyzuje tworzenie punktów przywracania.*

Oprogramowanie CyberSense domyślnie analizuje pliki i bazy danych. Użytkownicy nie muszą ręcznie poddawać migawek kwarantannie. **CyberSense przeprowadza swoją analizę bez konieczności wykonywania przez użytkownika własnych badań pod kątem zagrożeń, a ponadto automatyzuje tworzenie punktów przywracania.**[104]

Rozwiązanie Rubrik RSC w trybie zarządzania „tylko RSC" stanowi pojedyncze miejsce awarii dla wielu funkcji. Najbardziej niepokojące jest to, że atak może spowodować zakłócenie działania usługi RSC, które wpłynie na łączność internetową użytkownika lub łączność między lokalizacją użytkownika a usługą RSC. Po takich atakach użytkownicy mają do dyspozycji w ramach rozwiązania ograniczony zestaw funkcji, dostępnych za pośrednictwem interfejsu użytkownika Rubrik CDM lub automatyzacji opartej na interfejsach API, ale tylko wtedy, gdy utworzyli konto usługi RSC przed atakiem.[105, 106] Organizacja może przywrócić następujące obciążenia robocze i dane bez korzystania z usługi RSC: MongoDB, Microsoft Exchange, pliki, migawki funkcji Hyper-V, Live Mount z woluminów zarządzanych, pliki hosta NAS, Oracle, SQL Server, VCD i VMware.[107] Przywracanie systemu SAP HANA bez korzystania z usługi RSC wymaga narzędzi innych firm, takich jak Studio i Cockpit Cross, oraz wsparcia firmy Rubrik za pośrednictwem tunelu wsparcia. Przywracanie bazy danych IBM Db2 bez korzystania z usługi RSC również wymaga narzędzi firmy IBM oraz wsparcia firmy Rubrik za pośrednictwem tunelu wsparcia.[108]

Fizyczna izolacja

NIST definiuje fizyczną izolację jako „interfejs między dwoma systemami, w którym (a) nie są one połączone fizycznie i (b) żadne połączenie logiczne nie jest zautomatyzowane (tj. dane są przesyłane przez interfejs tylko ręcznie, pod kontrolą człowieka)".[109]

Fizyczne izolacje mogą pomóc w kontrolowaniu przepływu danych od źródła do celu i mogą być ważnym elementem każdej strategii ochrony przed oprogramowaniem ransomware i Cyber Recovery. Jeśli atak lub zdarzenie zagrozi produkcyjnym systemom tworzenia kopii zapasowych, możliwość zablokowania ruchu z systemów produkcyjnych do chronionych kopii zapasowych w sejfach Cyber Recovery może zapewniać zabezpieczenie przed awarią.

Separacja fizyczna

Przykład rozwiązania separacji fizycznej można było zobaczyć w filmie Mission Impossible, w którym główny bohater musiał ominąć wszystkie inne zabezpieczenia obiektu, aby uzyskać dostęp do poufnych danych w systemie komputerowym, który nie był podłączony do żadnej sieci zewnętrznej. Separacja fizyczna może również korzystać z normalnie rozłączonych segmentów dedykowanej sieci fizycznej do przesyłania kopii zapasowych z systemów produkcyjnych do sejfu. Po rozłączeniu taka operacyjna fizyczna izolacja tworzą fizyczną barierę, której dane nie mogą przekroczyć automatycznie, co utrudnia cyberprzestępcom dostęp do nich.

Organizacje mogą fizycznie odizolować rozwiązanie Dell PowerProtect Cyber Recovery, aby umożliwić realizację strategii operacyjnej fizycznej izolacji. Rozwiązanie korzysta z dedykowanego połączenia fizycznego i wykonuje replikację danych jako operację pobierania z sejfu, a nie operację wysyłania z rozwiązania do tworzenia kopii zapasowych. Podczas kopiowania/replikacji rozwiązanie aktywuje połączenie, szyfruje dane i przesyła je przez dedykowaną linię.[110] Po zakończeniu replikacji rozwiązanie ponownie wyłącza połączenie po stronie sejfu. Rozwiązanie zapewnia niezmienność kopii w sejfie dzięki zasadom blokady przechowywania, a więc nawet jeśli użytkownik lub system uzyska dostęp, to nie może zmodyfikować ani usunąć kopii przechowywanych w sejfie. Żaden ruch związany z zarządzaniem nie przechodzi

przez ścieżkę replikacji, więc **nawet jeśli cyberprzestępcy przejmą kontrolę nad lokalnym rozwiązaniem do tworzenia kopii zapasowych, sejf inicjuje i rozłącza ścieżkę replikacji oraz używa jednokierunkowego pobierania tylko danych ze źródła danych, ograniczając w ten sposób bezpośredni dostęp do sejfu.**[111]

Izolacja logiczna

Z drugiej strony izolacja logiczna wykorzystuje systemy, które mogą znajdować się w tej samej sieci fizycznej, ale tworzy logiczną separację i umożliwia kontrolę sieci, aby systemy nie mogły przesyłać danych między sobą. Rozwiązanie wykorzystuje dodatkowe implementacje zabezpieczeń, takie jak szyfrowanie i haszowanie wraz z RBAC i uwierzytelnianiem wieloskładnikowym, aby żaden nieautoryzowany system lub użytkownik nie mógł odczytać danych znajdujących się w innym systemie.

Firma Rubrik opisuje swoją funkcję Cyber Recovery jako wykorzystanie logicznej strategii fizycznej izolacji.[112, 113] Wiele z dostępnych publicznych deklaracji firmy Rubrik podaje w wątpliwość konieczność stosowania fizycznej izolacji. Prezentacja firmy Rubrik zatytułowana „Rubrik Security – Air Gap and Immutability" zawiera stwierdzenie, że jej natywne rozwiązanie jest odizolowane fizycznie, ponieważ nie ma możliwości uzyskania dostępu do kopii zapasowych ani ich edycji, gdy rozwiązanie je wykona, mimo że urządzenie Rubrik pozostaje w sieci fizycznej.[114] Jednak uwierzytelniony cyberprzestępca może nadal uzyskać dostęp do graficznego interfejsu użytkownika urządzenia, co może mieć konsekwencje dla odzyskania danych. Aby temu zapobiec, firma Rubrik stosuje blokady przechowywania, które zapobiegają wygaśnięciu kopii zapasowych, co czyni je niezmiennymi. Po włączeniu blokady przechowywania uniemożliwiają również przywrócenie ustawień fabrycznych i wyczyszczenie klastra Rubrik. Zgodnie z przewodnikiem po zabezpieczeniach Rubrik CDM, rozwiązanie domyślnie wyłącza globalnie blokady przechowywania w klastrze i wymaga od klientów skontaktowania się z działem wsparcia firmy Rubrik w celu ich włączenia.[115] Publicznie dostępne źródła nie wyjaśniają, czy dział wsparcia firmy Rubrik może również wyłączyć blokady przechowywania, co grozi tym, że autoryzowany cyberprzestępca może nadal być w stanie ominąć warstwy zabezpieczeń.

> *Żaden ruch związany z zarządzaniem nie przechodzi przez ścieżkę replikacji, więc nawet jeśli cyberprzestępcy przejmą kontrolę nad lokalnym rozwiązaniem do tworzenia kopii zapasowych, sejf inicjuje i rozłącza ścieżkę replikacji oraz używa jednokierunkowego pobierania tylko danych ze źródła danych, ograniczając w ten sposób bezpośredni dostęp do sejfu.*

Wnioski

Organizacje muszą aktywnie brać pod uwagę liczne wektory ataków na ich centra danych. Dobry plan ochrony danych ma na celu ochronę wszystkich danych, a w szczególności danych krytycznych niezbędnych do prowadzenia działalności. Przeanalizowaliśmy publicznie dostępne informacje dotyczące rozwiązań Dell PowerProtect Cyber Recovery i Rubrik Secure Cloud, aby sprawdzić, jak oba rozwiązania podchodzą do zarządzania, ochrony i odzyskiwania danych.

Rozwiązanie PowerProtect Cyber Recovery fizycznie izoluje kopie zapasowe krytycznych danych w sejfie i zapewnia możliwość ich odzyskania po cyberataku. Rozwiązanie wykorzystuje operacyjną strategię fizycznej izolacji i separacji, czego rozwiązanie Rubrik Secure Cloud nie oferuje — opiera się jedynie na izolacji logicznej.

Cyber Recovery wykorzystuje analitykę opartą na uczeniu maszynowym w silniku CyberSense w celu oceny integralności danych w sejfie i identyfikowania czystych danych kopii zapasowych do odzyskania. Z kolei rozwiązanie Rubrik Secure Cloud oferuje narzędzie analityczne wytrenowane przez uczenie maszynowe, które szuka anomalii, zamiast przeprowadzać głębokie skanowanie plików.

Co więcej, rozwiązanie Cyber Recovery oferuje wiele opcji odzyskiwania, wykorzystując nienaruszone dane z sejfu, aby ułatwić sprawne i bezproblemowe przywrócenie działalności. W wielu przypadkach rozwiązanie PowerProtect Cyber Recovery może wykorzystać funkcje i zalety, których brakuje rozwiązaniu Rubrik Secure Cloud, stanowiąc dzięki temu potencjalnie bezpieczniejsze rozwiązanie zdolne do głębszej analizy w celu zminimalizowania przestojów i przyspieszenia odzyskiwania.

---

1. Anastasia Dergacheva i Jesse R. Taylor, „Study Finds Average Cost of Data Breaches Continued to Rise in 2023”, dostęp 25 lipca 2024 r., https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/03/study-finds-average-cost-of-data-breaches-continued-to-rise-in-2023.
2. Dell, „Przewodnik po rozwiązaniu Dell PowerProtect Cyber Recovery”, dostęp 18 kwietnia 2024 r., https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
3. Dell, „Przewodnik po rozwiązaniu Dell PowerProtect Cyber Recovery”.
4. Rubrik, „Rubrik Security Cloud Architecture and Security Implementation”, dostęp 18 kwietnia 2024 r., https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.
5. Rubrik, „Rubrik Security Cloud Architecture and Security Implementation”, dostęp 18 kwietnia 2024 r., https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.
6. Rob Emsley, „Public Cloud Vault to Secure, Isolate and Recover Data”, dostęp 20 marca 2024 r., https://www.dell.com/en-us/blog/public-cloud-vault-to-secure-isolate-and-recover-data/.

7. Brian White, „Dell's PowerProtect Cyber Recovery Expands to Microsoft Azure", dostęp 20 marca 2024 r., https://www.dell.com/en-us/blog/dells-powerprotect-cyber-recovery-expands-to-microsoft-azure/.
8. Dell, „Cyber Recovery on Google Cloud Platform", dostęp 20 marca 2024 r., https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-cyber-recovery-reference-architecture/cyber-recovery-on-google-cloud-platform/.
9. Chris Mellor, „Up to $5m compensation if Rubrik Cloud Vault recovery busted", dostęp 20 marca 2024 r., https://blocksandfiles.com/2022/02/24/up-to-5m-compensation-if-rubrik-cloud-vault-recovery-busted/.
10. Kristina Avrionova, „Frequently Asked Questions about Rubrik Cloud Vault", dostęp 20 marca 2024 r., https://www.rubrik.com/blog/company/22/3/faq-about-rubrik-cloud-vault.
11. Chris Wahl, „Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture", dostęp 22 marca 2024 r., https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
12. Dell, „Data Domain Invulnerability Architecture: Enhancing Data Integrity and Recoverability", dostęp 7 czerwca 2024 r., https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h7219-data-domain-data-invul-arch-wp.pdf.
13. Dell, „Consolidate Governance and Compliance Archive Data", dostęp 4 kwietnia 2024 r., https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-domain-retention-lock/consolidate-governance-and-compliance-archive-data/.
14. Dell, „Przewodnik po rozwiązaniu Dell PowerProtect Cyber Recovery", dostęp 24 marca 2024 r., https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
15. Rubrik, „Retention-locked SLA Domain attributes", dostęp 2 kwietnia 2024 r., https://docs.rubrik.com/en-us/8.0/ug/cdm/attributes_of_retention_locked_sla_domains.html.
16. Rubrik, „Rubrik Cyber Recovery", dostęp 20 marca 2024 r., https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/brf-rubrik-cyber-recovery.pdf.
17. Rubrik, „Rubrik Licensing: Subscribe to Simplicity", dostęp 20 marca 2024 r., https://www.rubrik.com/content/dam/rubrik/en/resources/data-sheet/rubrik-licensing-data-sheet.pdf.
18. Rubrik, „Workloads require third-party tools for recovery", dostęp 6 maja 2024 r., https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.
19. Rubrik, „Recoverable workloads during RSC service disruption", dostęp 6 maja 2024 r., https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.
20. Rubrik, „Workloads require third-party tools for recovery".
21. Dell, „Strengthen your security posture with Managed Detection and Response", dostęp 2 kwietnia 2024 r., https://www.delltechnologies.com/asset/pl-pl/services/managed-services/technical-support/managed-detection-and-response-datasheet.pdf.
22. Dell, „Instrukcja instalacji Dell PowerProtect Cyber Recovery 19.13", dostęp 20 marca 2024 r., https://www.dell.com/support/manuals/en-us/cyber-recovery/irs_p_19.13_installation/installing-the-cyber-recovery-software?guid=guid-8718978d-ddd0-4dc0-bca7-fb04a2f3d1fb&lang=en-us.
23. Dell, „Instrukcja instalacji Dell PowerProtect Cyber Recovery 19.13".
24. Dell, „Instrukcja instalacji Dell PowerProtect Cyber Recovery 19.13".
25. Dell, „Installing CyberSense in Dell PowerProtect Cyber Recovery", dostęp 20 marca 2024 r., https://infohub.delltechnologies.com/en-US/l/ransomware-protection-secure-your-data-on-dell-powerflex-with-powerprotect-cyber-recovery-1/installing-cybersense-in-dell-powerprotect-cyber-recovery-1/.
26. Dell, „Przewodnik po rozwiązaniu Dell PowerProtect Cyber Recovery".
27. Rubrik, „Downloading and installing Rubrik CDM", dostęp 20 marca 2024 r., https://docs.rubrik.com/en-us/saas/install/download_install_cdm_on_appliance_nodes.html.
28. Rubrik, „Setting up a Rubrik cluster using the UI", dostęp 20 marca 2024 r., https://docs.rubrik.com/en-us/saas/install/setting_up_ui.html.
29. Rubrik, „Setting up a Rubrik cluster using the CLI", dostęp 20 marca 2024 r., https://docs.rubrik.com/en-us/saas/install/setting_up_cli.html.
30. Rubrik, „Registering Rubrik clusters using the online method", dostęp 20 marca 2024 r., https://docs.rubrik.com/en-us/saas/install/registering_clusters_online.html.
31. Rubrik, „Registering Rubrik clusters using the offline method", dostęp 2 kwietnia 2024 r., https://docs.rubrik.com/en-us/saas/install/registering_clusters_offline.html.
32. Rubrik, „Enabling MFA", dostęp 21 marca 2024 r., https://docs.rubrik.com/en-us/saas/install/rsc_enabling_mfa.html.
33. Rubrik, „Adding the initial account", dostęp 21 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/adding_the_initial_account.html.
34. TrustRadius, „Learning Rubrik by putting the pieces together Brik by Brik", dostęp 21 marca 2024 r., https://www.trustradius.com/reviews/rubrik-2023-09-20-21-03-04.
35. Dell, „Przewodnik po rozwiązaniu Dell PowerProtect Cyber Recovery".

36. Index Engines, „CyberSense®: How it Works", dostęp 21 marca 2024 r., https://www.indexengines.com/how-it-works.
37. Rubrik, „Anomaly event details", dostęp 21 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/anomaly_event_details.html.
38. Rubrik, „Events page", dostęp 21 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/common/events_page.html.
39. Rubrik, „RSC Data Threat Analytics", dostęp 21 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/ri_ransomware_monitoring.html.
40. Rubrik, „RSC Data Threat Analytics".
41. Dell Technologies, „Dell PowerProtect Cyber Recovery: Reference Architecture", dostęp 6 maja 2024 r., https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h18661-dell-powerprotect-cyber-recovery-reference-architecture-wp.pdf.
42. Dell Technologies, „Dell EMC Avamar for Hyper-V", dostęp 16 maja 2024 r., https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu89876.pdf.
43. Dell Technologies, „Dell EMC NetWorker Module for Microsoft for Hyper-V", dostęp 16 maja 2024 r., https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu92011.pdf.
44. VMware, „Accelerate IT. Innovate with your cloud.", 9 maja 2024 r., https://www.vmware.com/files/pdf/VMware-Corporate-Brochure-BR-EN.pdf.
45. Statista, „Cloud infrastructure services vendor market share worldwide from fourth quarter 2017 to first quarter 2024", 17 lipca 2024 r., https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/.
46. Rubrik, „RSC Data Threat Analytics".
47. Dell Technologies, „CyberSense® for PowerProtect Cyber Recovery", dostęp 27 czerwca 2024 r., https://www.delltechnologies.com/asset/en-gb/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
48. Rubrik, „RSC Data Threat Analytics".
49. Index Engines, „CyberSense® Support Matrix", dostęp 21 marca 2024 r., https://www.indexengines.com/csmatrix.
50. Dell Technologies, „CyberSense® for PowerProtect Cyber Recovery".
51. Rubrik, „Keep Your Databases Running in the Face of Any Threat".
52. Index Engines, „CyberSense® Support Matrix".
53. Dell Technologies, „Dell EMC Avamar for Hyper-V".
54. Dell Technologies, „Dell EMC NetWorker Module for Microsoft for Hyper-V".
55. Rubrik, „Anomaly incidents", dostęp 2 kwietnia 2024 r., https://docs.rubrik.com/en-us/saas/saas/anomaly_incident.html.
56. Rubrik, „Data Threat Analytics events", dostęp 2 kwietnia 2024 r., https://docs.rubrik.com/en-us/saas/saas/ri_events.html.
57. Rubrik, „Viewing Anomaly Detection", dostęp 2 kwietnia 2024 r., https://docs.rubrik.com/en-us/saas/saas/viewing_ri_investigations.html.
58. Rubrik, „VM Encryption Detection", dostęp 2 kwietnia 2024 r., https://docs.rubrik.com/en-us/saas/saas/vm_encryption_detection.html.
59. Rubrik, „Viewing the Threat Monitoring page", 2 kwietnia 2024 r., https://docs.rubrik.com/en-us/saas/saas/viewing_the_threat_monitoring_page.html.
60. Rubrik, „Initiating a threat hunt", dostęp 2 kwietnia 2024 r., https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
61. Rubrik, „Quarantining matched files or objects", dostęp 2 kwietnia 2024 r., https://docs.rubrik.com/en-us/saas/saas/quarantining_matched_objects_or_files.html.
62. Dell, „CyberSense® for PowerProtect Cyber Recovery".
63. Dell, „CyberSense® for PowerProtect Cyber Recovery".
64. Index Engines, „The Power of CyberSense's Machine Learning", dostęp 2 kwietnia 2024 r., https://go.indexengines.com/csmachinelearning.
65. Index Engines, „The Power of CyberSense's Machine Learning".
66. Index Engines, „The Power of CyberSense's Machine Learning".
67. Dell, „CyberSense® for PowerProtect Cyber Recovery".
68. Rubrik, „Anomaly Detection behavioral model", dostęp 20 maja 2024 r., https://docs.rubrik.com/en-us/saas/saas/anomaly_detection_behavioral_model.html.
69. Amazon, „Training ML Models", dostęp 2 kwietnia 2024 r.,https://docs.aws.amazon.com/machine-learning/latest/dg/training-ml-models.html.
70. Rubrik, „Defense in Depth with Polaris Radar", dostęp 21 marca 2024 r., https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/Defense-In-Depth-Polaris-Radar-Technical-White-Paper.pdf.
71. Rubrik, „Data Threat Analytics dashboard", dostęp 21 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/ri_dashboard.html.
72. Rubrik, „Initiating a threat hunt", dostęp 21 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
73. SentinelOne, „What Is A Malware File Signature (And How Does It Work)?" dostęp 4 kwietnia 2024 r., https://www.sentinelone.com/blog/what-is-a-malware-file-signature-and-how-does-it-work/.

74. Rubrik, „Threat hunts", dostęp 21 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/ri_threat_hunts.html.
75. Rubrik, „Anomaly Detection features", dostęp 22 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
76. Rubrik, „Behavioral model".
77. Index Engines, „The Power of CyberSense's Machine Learning".
78. Dell, „CyberSense® for PowerProtect Cyber Recovery".
79. Rubrik, „Behavioral model".
80. Rubrik, „Anomaly Detection features".
81. Rubrik, „Behavioral model".
82. Dell, „CyberSense® for PowerProtect Cyber Recovery".
83. Morningstar, „Index Engines' CyberSense Announces 99.99% SLA in Detecting Ransomware Corruption, Empowering Smarter Recovery", dostęp 17 lipca 2024 r., https://www.morningstar.com/news/pr-newswire/20240618ny41171/index-engines-cybersense-announces-9999-sla-in-detecting-ransomware-corruption-empowering-smarter-recovery.
84. Rubrik, „Threat Monitoring", dostęp 22 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/threat_monitoring.html.
85. Index Engines, „The Power of CyberSense's Machine Learning".
86. Index Engines, „The Power of CyberSense's Machine Learning".
87. Rubrik, „Anomaly Detection features", dostęp 22 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
88. Index Engines, „The Power of CyberSense's Machine Learning".
89. Rubrik, „Investigating and recovering anomalous files for filesets", dostęp 22 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files.html.
90. Rubrik, „Investigating and recovering anomalous files for virtual machines", dostęp 22 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files_for_virtual_machines.html.
91. Rubrik, „Full snapshot recovery of a virtual machine", dostęp 22 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/full_snapshot_recovery_of_a_virtual_machine.html.
92. Rubrik, „Recovery of a batch of virtual machines", dostęp 22 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
93. Rubrik, „Performing bulk recovery for Recovery Plans", dostęp 22 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/performing_bulk_recovery_for_recoveryplans.html.
94. Rubrik, „Recovery of a batch of virtual machines", dostęp 4 kwietnia 2024 r., https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
95. Rubrik, „Recovery of virtual machines", dostęp 16 kwietnia 2024 r., https://docs.rubrik.com/en-us/saas/saas/vs_recovery_vm.html.
96. Odzyskany magazyn danych zazwyczaj znajduje się w klastrze Rubrik, a nie w środowisku produkcyjnym.
97. Rubrik, „Recovery of a batch of virtual machines", dostęp 16 kwietnia 2024 r., https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
98. Dell, „Restore plan", dostęp 16 kwietnia 2024 r., https://infohub.delltechnologies.com/en-US/l/powerprotect-data-manager-protection-for-vmware-cloud-foundation-on-dell-emc-vxrail-1/restore-plan/.
99. Dell, „PowerProtect Data Manager overview", dostęp 16 kwietnia 2024 r., https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-manager-deployment-best-practices-1/powerprotect-data-manager-overview-4/.
100. Dell, „PowerProtect Data Manager 19.9 Administration and User Guide", dostęp 16 kwietnia 2024 r., https://www.dell.com/support/manuals/en-us/enterprise-copy-data-management/pp-dm_19.9_ag/file-level-restore-of-a-powerprotect-backup-in-the-vsphere-client.
101. Dell, „Recovery Orchestration with PowerProtect Data Manager Overview", dostęp 16 kwietnia 2024 r., https://www.youtube.com/watch?v=po2oMnAg_x4.
102. Rubrik, „Quarantine files or objects", dostęp 24 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/quarantine.html.
103. Rubrik, „Downloading quarantined files for forensic analysis", dostęp 24 marca 2024 r., https://docs.rubrik.com/en-us/saas/saas/downloading_quarantined_files_for_forensic_analysis.html.
104. Forrester, „The Total Economic Impact™ Of Dell PowerProtect Cyber Recovery", dostęp 16 kwietnia 2024 r., https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/the-total-economic-impact-dell-powerprotect-cyber-recovery.pdf.
105. Rubrik, „Workload recovery during an RSC service disruption", dostęp 16 kwietnia 2024 r., https://docs.rubrik.com/en-us/saas/saas/workload_recovery_during_rsc_outage.html.
106. Rubrik, „Rubrik CDM APIs and service account workflows", dostęp 16 kwietnia 2024 r., https://docs.rubrik.com/en-us/saas/saas/rubrik_apis_sa_workflows.html.
107. Rubrik, „Recoverable workloads during RSC service disruption", dostęp 16 kwietnia 2024 r., https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.

108. Rubrik, „Workloads require third-party tools for recovery", dostęp 16 kwietnia 2024 r., https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.

109. NIST, „Computer Security Resource Center Glossary: air gap", dostęp 29 lipca 2024 r., https://csrc.nist.gov/glossary/term/air_gap.

110. Dell, „Przewodnik po rozwiązaniu Dell PowerProtect Cyber Recovery".

111. Dell, „Dell PowerProtect Cyber Recovery: Reference Architecture".

112. Adam Eckerle, „Debunking the Myths about Air Gaps", dostęp 14 marca 2024 r., https://www.rubrik.com/blog/technology/2021/11/debunking-the-myths-about-air-gaps.

113. Rubrik, „Air-Gap, Isolated Recovery, and Ransomware - Cost vs. Value", dostęp 14 marca 2024 r., https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/Air-Gap-Isolated-Recovery-and-Ransomware-Cost-vs.-Value.pdf.

114. Brian Williams, „Rubrik Air Gap and Immutability", dostęp 14 marca 2024 r., https://vimeocom/561870246.

115. Rubrik, „Retention locks in the Rubrik cluster", dostęp 18 marca 2024 r., https://docs.rubrik.com/en-us/9.0/sg/security_guide/retention_locks_in_the_rubrik_cluster.html.

▶ Zobacz oryginalną, angielską wersję tego raportu

Projekt ten został zlecony przez Dell Technologies.

Principled Technologies®

Facts matter.®