Zwiększ cyberodporność i chroń dane przed zagrożeniami typu cyber ransomware, korzystając m.in. z odizolowanego sejfu i oprogramowania do analizy bazującego na uczeniu maszynowym opartym na sztucznej inteligencji

Dzięki rozwiązaniu PowerProtect Cyber Recovery z CyberSense firmy Dell Technologies

W miarę wzrostu częstotliwości zagrożeń cybernetycznych i ewoluowaniu metod ataków plany ochrony danych muszą uwzględniać podejście, które zapewnia bezpieczeństwo i analizowanie wszystkich komponentów IT: od najmniej ważnych do najistotniejszych. Dell PowerProtect Cyber Recovery może pomóc w ochronie najbardziej poufnych danych o znaczeniu krytycznym, a zarazem zapewnić prawidłowe odzyskiwanie danych w obliczu cyberataku lub innego zakłócającego zdarzenia.

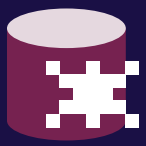
Dell PowerProtect Cyber Recovery to rozwiązanie do zarządzania danymi oraz ich ochrony i odzyskiwania, które pomaga organizacjom chronić dane i aplikacje przed atakami ransomware, niszczycielskimi cyberatakami i nieoczekiwanymi zdarzeniami. W rozwiązaniu tym stosuje się metodę wielokrotnego kopiowania, która polega na tym, że po utworzeniu kopii zapasowych kopiuje się je do izolowanej pamięci masowej w celu ochrony i analizy. Rozwiązanie PowerProtect Cyber Recovery składa się z wielu komponentów, w tym z co najmniej jednego sejfu pamięci masowej znajdującego się potencjalnie lokalnie w urządzeniu PowerProtect DD (nazywanym wcześniej Data Domain) lub w chmurze za pośrednictwem zdefiniowanej programowo pamięci masowej Dell APEX Protection Storage for Public Cloud (nazywanej wcześniej DD Virtual Edition). W obu przypadkach sejf jest fizycznie i operacyjnie odizolowany, tj. oddzielony od środowiska produkcyjnego — potencjalnie fizycznie oddzielony w przypadku środowiska lokalnego i logicznie oddzielony w przypadku środowiska APEX. To sprawia, że złośliwym podmiotom i nieupoważnionym użytkownikom niezwykle trudno jest się zalogować i naruszyć kopie zapasowe.

PowerProtect Cyber Recovery obejmuje też CyberSense, czyli w pełni zautomatyzowany i zintegrowany silnik inteligentnej analizy zabezpieczeń, który automatycznie skanuje dane, pliki, bazy danych i obrazy w sejfie w poszukiwaniu oznak uszkodzenia w wyniku ataku ransomware. CyberSense zapewnia pełną analizę treści, przyjmuje obserwacje z plików, które służą jako dane wejściowe dla modelu uczenia maszynowego (ML) opartego na sztucznej inteligencji (SI) oraz wykrywa złośliwe działania obejmujące masowe usuwanie, szyfrowanie i wprowadzanie innych podejrzanych zmian w infrastrukturze podstawowej (w tym w usłudze Active Directory i DNS), plikach użytkowników oraz produkcyjnych bazach danych o znaczeniu krytycznym, które mogą wskazywać na atak ransomware lub niszczycielski. Gdy CyberSense wykryje wzorce uszkodzenia, generuje na pulpicie nawigacyjnym PowerProtect Cyber Recovery alert, który zawiera dodatkowe informacje na temat skali i wpływu ataku.[1]

PowerProtect Cyber Recovery pomaga organizacjom łagodzić skutki cyberataków, zwiększać odporność danych dzięki ich wielu kopiom zapasowym z osobnych lokalizacji, skracać przestoje i utrzymywać ciągłość prowadzenia działalności biznesowej. W niniejszym raporcie wykorzystano dostępne publicznie informacje w celu podkreślenia kluczowych cech i funkcji w zakresie ochrony danych oraz przedstawiono nasze wnioski z analizy porównawczej silnika CyberSense.

Ochrona poufnych danych

Szyfrowanie niezmiennych danych w locie podczas replikacji kopii zapasowych do fizycznie i logicznie odizolowanych sejfów



Wykrywanie uszkodzenia strony programu SQL Server

Silnik CyberSense wykrył zarażenie, którego nie zgłosiło konkurencyjne rozwiązanie

Wykrywanie nieuszkodzonych kopii zapasowych

Silnik CyberSense wykrył najnowszą niezarażoną kopię zapasową na potrzeby odzyskiwania danych

Bezpieczeństwo

Dell PowerProtect Cyber Recovery udostępnia kilka funkcji zabezpieczeń, które pomagają chronić dane o znaczeniu krytycznym przed atakami ransomware i innymi wyrafinowanymi zagrożeniami, uniemożliwiają nieupoważnionym użytkownikom uzyskanie dostępu do poufnych informacji oraz przyspieszają odzyskiwanie danych, dzięki czemu organizacje mogą szybko wznowić normalne działanie.

Cechy i funkcjonalność urządzeń PowerProtect DD mają kluczowe znaczenie dla działań w zakresie bezpieczeństwa, integralności i odzyskiwania danych, które realizują rozwiązania PowerProtect Cyber Recovery. Funkcje te obejmują:

1. **Niezmienność**
   Niezmienne dane nie mogą być modyfikowane ani usuwane, tylko zapisane. Systemy DD mogą zapisywać niezmienne kopie zapasowe zarówno w systemach produkcyjnych, jak i w Cyber Vault, co oznacza, że jeśli zły podmiot powinien w jakiś sposób uzyskać dostęp do systemu kopii zapasowych, nie może modyfikować, usuwać ani naruszać istniejących chronionych kopii.[2] Każda kopia zapasowa tworzona przez system DD w środowisku produkcyjnym staje się natychmiast niezmienna i dostępna do skopiowania do sejfu w celu zwiększenia bezpieczeństwa. W następnej sekcji tego raportu przyjrzymy się bardziej niezmienności.

2. **Blokada retencji**
   Funkcja DD Retention Lock sprawia, że dane są niezmienne przez wstępnie określony okres. Po umieszczeniu danych w blokadzie retencji żaden użytkownik ani system nie może zmieniać, usuwać ani modyfikować danych do momentu wygaśnięcia okresu blokady.[3]

   Blokada retencji ma tryby zarządzania i zgodności. Tryb zgodności umożliwia klientom spełnienie wielu standardów regulacyjnych. Niezależna strona trzecia zaświadczyła, że funkcja DD Retention Lock spełnia wymagania dotyczące pamięci masowej określone w regułach SEC 17a-4(f)(2) i 240.18a-6(e)(2) oraz regule FINRA 4511(c).[4] Ta funkcja może również pomóc w wspieraniu wysiłków organizacji w celu zapewnienia zgodności z przepisami FDA 21 CFR Part11, Sarbanes-Oxley Act, IRS 98025 i 97-22 i MoREQ2010 oraz standardem ISO 15489-1.[5]

   Ponieważ atakujący mogą próbować obejść blokadę retencji poprzez zmianę zegara systemowego, co spowodowałoby usunięcie plików wcześniej niż oczekiwano, DD ma wewnętrzny zegar bezpieczeństwa. System regularnie porównuje czasy zegarów bezpieczeństwa i systemowego. W przypadku skumulowanego dwutygodniowego odchylenia między tymi dwoma zegarami w jednym roku kalendarzowym system automatycznie wyłącza system plików DD (DDFS), aby zapobiec dostępowi do danych.[6]

3. **Szyfrowanie danych w locie za pomocą protokołu DDBoost**
   Dane w locie mogą stanowić poważne zagrożenie dla bezpieczeństwa. DDBoost ogranicza ilość danych w locie, umożliwiając serwerowi kopii zapasowych lub klientowi aplikacji wysyłanie tylko unikatowych segmentów danych, a nie wszystkich danych, w sieci do urządzenia DD. Ponadto organizacje mogą korzystać z protokołu DDBoost z certyfikatami lub bez nich do uwierzytelniania i szyfrowania danych. Certyfikaty zapewniają bezpieczniejszy transport danych. Szyfrowanie w locie umożliwia aplikacjom szyfrowanie kopii zapasowych w locie lub przywracanie danych przez sieć LAN z systemu. Klient może używać usług Transport Layer Services (TLS) do szyfrowania sesji między klientem a systemem.[7]

4. **Zabezpieczenia systemu operacyjnego DD (DD OS)**
   Funkcje zabezpieczeń DD obejmują również system operacyjny. DD OS wdraża niestandardowe mechanizmy kontroli dostępu i ograniczenia w powłoce Bash dla celów bezpieczeństwa. Tryb ograniczony powłoki Bash pozwala użytkownikom wykonywać tylko określony zestaw zdefiniowanych poleceń niezbędnych do wykonywania ich ról i zadań. System DD OS zwiększa integralność danych, blokując niezdefiniowane polecenia, które powodują nieautoryzowane lub niezamierzone modyfikacje systemu.[8]

5. **Kontrola dostępu oparta na rolach (RBAC) i zabezpieczenia systemu plików DD (DDFS)**
   Systemy DD używają kilku środków w celu ochrony plików i danych w systemie plików. Po pierwsze, systemy DD zapewniają kontrolę RBAC, która umożliwia administratorom definiowanie ról z określonymi uprawnieniami i przypisywanie użytkowników do tych ról. Tylko autoryzowani użytkownicy z odpowiednimi uprawnieniami mogą uzyskać dostęp do urządzenia i jego danych. Dzięki temu użytkownicy mają dostęp tylko do funkcji i danych potrzebnych do wykonywania swoich zadań, co zmniejsza ryzyko nieautoryzowanego dostępu lub przypadkowego narażenia na dane.

   DDFS używa również haszowania do weryfikacji integralności danych. Haszowanie przekształca dany klucz lub ciąg znaków w inną wartość. Urządzenie przechowuje unikatowe fragmenty danych w logicznych kontenerach pamięci masowej, a system plików zawiera skróty zarówno fragmentów danych, jak i kontenerów. Podczas pobierania danych system ponownie oblicza wartość skrótu danych, aby dopasować ją do wartości skrótu przechowywanego w DDFS, co pomaga upewnić się, że nic nie naruszyło danych ani nie uszkodziło ich.[9]

6. **Autoryzacja z dwiema rolami**
   Gdy organizacja włącza tryb zgodności DD Retention Lock, system DD zapewnia dodatkowe zabezpieczenia administracyjne w postaci podwójnego logowania. Oznacza to, że zarówno administrator systemu, jak i drugi autoryzowany użytkownik (np. kierownik ds. bezpieczeństwa) muszą się zalogować razem. Mechanizm podwójnego logowania w trybie zgodności DD Retention Lock działa jako zabezpieczenie przed wszelkimi działaniami, które mogą potencjalnie naruszyć integralność zablokowanych plików przed upływem okresu przechowywania.[10]

7. **Architektura Data Invulnerability**
   System operacyjny DD zapewnia kompleksową weryfikację, unikanie i ograniczanie błędów, ciągłe wykrywanie i naprawianie błędów oraz odzyskiwanie systemu plików w celu ochrony przed problemami z integralnością danych spowodowanymi awariami sprzętu i oprogramowania. Kiedy system DD otrzymuje żądania zapisu z oprogramowania do tworzenia kopii zapasowych, najpierw analizuje segment danych pod kątem nadmiarowości, obliczając odcisk palca dla segmentu danych i porównując go z istniejącymi odciskami palców przechowywanymi w systemie. Przechowuje na dysku tylko unikatowe segmenty danych i ich odciski palców. Następnie DD stale odczytuje dane z dysku, ponownie oblicza odcisk palca, który odczytuje, i upewnia się, że jest zgodny z odciskiem palca na dysku. System DD przeprowadza proces autonaprawy w celu odtworzenia uszkodzonych danych i przywrócenia danych do prawidłowego stanu, jeśli system wykryje uszkodzenie podczas tego procesu (tj. jeśli odczyty z powrotem nie są zgodne z zapisanymi danymi). Ponadto proces autonaprawy pomaga chronić system przed innymi zmianami, które mogą mieć wpływ na integralność platformy.

Niezmienność*

Dzięki skonfigurowaniu kopii zapasowych jako niezmiennych, czyli przeznaczonych tylko do odczytu, organizacja może z pełnym zaufaniem używać tych kopii do odzyskiwania danych. Pod względem operacyjnym niezmienność pomaga zachować autentyczność i niezawodność danych.

* 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.

Zasada działania

Systemy DD zapewniają niezmienność sposobu przechowywania danych przy użyciu MTree. MTree to partycje logiczne systemu plików. Gdy aplikacja zapisuje dane w MTree, system DD używa funkcji o nazwie Fast Copy, aby utworzyć kopię oryginalnego MTree z punktu w czasie do nowego MTree. W nowym drzewie MTree DD stosuje blokadę retencji, aby upewnić się, że użytkownik lub proces nie może usunąć nowego drzewa MTree przez czas określony przez okres przechowywania. Nowe MTree jest niezmienną kopią danych i jest niezależne od oryginalnego MTree.[11]

Rozwiązania PowerProtect Cyber Recovery korzystają również z replikacji MTree do kopiowania niezmiennych kopii danych z produkcyjnego urządzenia DD na inne urządzenie DD w sejfie za pośrednictwem protokołu DDBoost.[12] Podczas początkowej synchronizacji między dwoma DD rozwiązanie kopiuje wszystkie dane do DD sejfu. Każda kolejna synchronizacja będzie kopiować tylko nowe i zmienione segmenty danych. CyberSense, które omówimy w dalszej części tego raportu, skanuje wszystkie niezmienne kopie w magazynie pod kątem potencjalnego uszkodzenia.

Podejście do niezmienności

Konieczność usunięcia niezmiennych kopii zapasowych jest rzadka, ale taki scenariusz się zdarza. rganizacje mogą potencjalnie napotkać problemy związane z pojemnością i wynikającymi z tego kosztami po zgromadzeniu niezmiennych kopii zapasowych, których nie mogą usunąć. Przechowywanie kopii zapasowych może wymagać dużej pojemności, co z kolei wymaga bieżących kosztów operacyjnych, zarządzania i monitorowania oprócz początkowej inwestycji w sprzęt. Okresowe usuwanie niezmiennych kopii zapasowych może pomóc w rozwiązaniu tych problemów.

Jak już zauważyliśmy, rozwiązanie Dell PowerProtect Cyber Recovery zapewnia niezmienność dzięki wykorzystaniu blokady retencji i innych narzędzi. Blokada retencji zapewnia pewną elastyczność, ponieważ oba tryby, Compliance i Governance, oferują niewielkie modyfikacje w sposobie wdrażania niezmienności przez klientów. Niezmienność oznacza, że użytkownicy ani złośliwe podmioty nie mogą usuwać kopii zapasowych, ale w niektórych przypadkach, takich jak problemy z pojemnością pamięci masowej, rozwiązanie PowerProtect Cyber Recovery umożliwia klientom usunięcie ich w trybie Retention Lock — Governance.

Jak wypadają podobne produkty innych firm w porównaniu z rozwiązaniem PowerProtect Cyber Recovery? Przeanalizowaliśmy publicznie dostępne informacje dotyczące rozwiązań Cohesity Cyber Recovery, Veeam, Rubrik i Veritas NetBackup. Oprócz Cohesity Cyber Recovery, rozwiązania mogą być zainstalowane zarówno w lokalizacji, jak i poza nim (Cohesity to rozwiązanie oparte na chmurze, obsługiwane przez AWS). Dokumentacja dotycząca czterech rozwiązań twierdzi, że zapewniają one niezmienność, ale warto zauważyć, że rozwiązania Rubrik i NetBackup różnią się od PowerProtect Cyber Recovery.

W przypadku rozwiązania Rubrik administratorzy mogą usuwać kopie zapasowe, ale nie od strony klienta i tylko z zastosowaniem określonych elementów kontroli. Ponadto wszystkie zapisy są „poza miejscem", co oznacza, że nowe zapisy nigdy nie dotykają zapisanych wcześniej danych.[13]

Pomimo niezmienności administratorzy lub złośliwe podmioty mogą usunąć blokadę kopii zapasowych w pamięci masowej z obsługą NetBackup WORM. Następnie mogą usunąć obraz za pomocą polecenia bpexdate.[14]

Izolacja

Izolacja danych odnosi się do odseparowywania danych i ograniczania dostępu do nich dzięki barierom lub granicom, które zapobiegają nieupoważnionemu dostępowi. Izolacja używa tymczasowych połączeń sieciowych zamiast połączeń trwałych.

Izolacja danych zapewnia brak styczności danych o znaczeniu krytycznym z zarażoną siecią, w której złośliwy podmiot mógłby podjąć próbę zmiany konfiguracji, usunięcia danych, modyfikacji zasad lub podsłuchiwania ruchu sieciowego w poszukiwaniu danych uwierzytelniających użytkowników. Izolacja pomaga też zmniejszyć obszar narażony na ataki, ograniczając złośliwym podmiotom możliwości uzyskania dostępu i kontroli. Ponadto organizacje mogą ograniczać krąg użytkowników, którzy mają dostęp, tylko do autoryzowanego personelu, co pomaga zapobiegać nadpisywaniu danych przez nieupoważnione osoby.

Oprócz wspomnianych już funkcji PowerProtect Cyber Recovery może zapewniać izolację fizyczną i logiczną, aby pomagać w ochronie danych. Rozwiązanie PowerProtect Cyber Recovery może wykorzystywać zarówno fizyczną izolację, w której dane kopii zapasowej są fizycznie odłączone od sieci produkcyjnej i przechowywane w odizolowanej lokalizacji, jak i logiczną izolację, która polega na elementach kontroli dostępu do sieci w celu oddzielenia logicznie odłączonych kopii zapasowych od środowiska produkcyjnego. Posiadanie dwóch typów izolacji jest cenne, ponieważ sama izolacja logiczna nie może powstrzymać użytkownika wewnętrznego z dostępem sieciowym do sejfu przed uzyskaniem dostępu i naruszeniem danych.

Odizolowane fizycznie lokalne urządzenie PowerProtect DD może działać jako sejf, w którym użytkownicy ani systemy ze środowiska produkcyjnego nie mogą uzyskiwać dostępu do komponentów. Sam sejf jest fizycznie odłączony od sieci produkcyjnej.[15] Dzięki eliminacji dostępu z sieci produkcyjnej do środowiska odzyskiwania danych organizacja może zmniejszyć obszar narażony na ataki. Jak wspomniano, dostęp do izolowanych danych wymaga oddzielnych poświadczeń bezpieczeństwa, a także uwierzytelniania wieloskładnikowego (MFA).[16]

Podejście do izolacji

Gartner stwierdza, że „izolowane środowiska odzyskiwania (IRES) z sejfami niezmiennych danych (IDV) zapewniają najwyższy poziom bezpieczeństwa i odzyskiwania danych wobec zagrożeń wewnętrznych, ransomware i innych form hakowania".[17] Firma zwraca również uwagę, że „IRE z IDV nie zastępuje, ale raczej uzupełnia tradycyjne systemy tworzenia kopii zapasowych i odtwarzania po awarii (DR), dostarczając trzecią niezmienną kopię zapasową w IRE wyposażonej we wszystkie narzędzia, procesy i zasoby do odzyskiwania systemów, których dotyczy problem".[18]

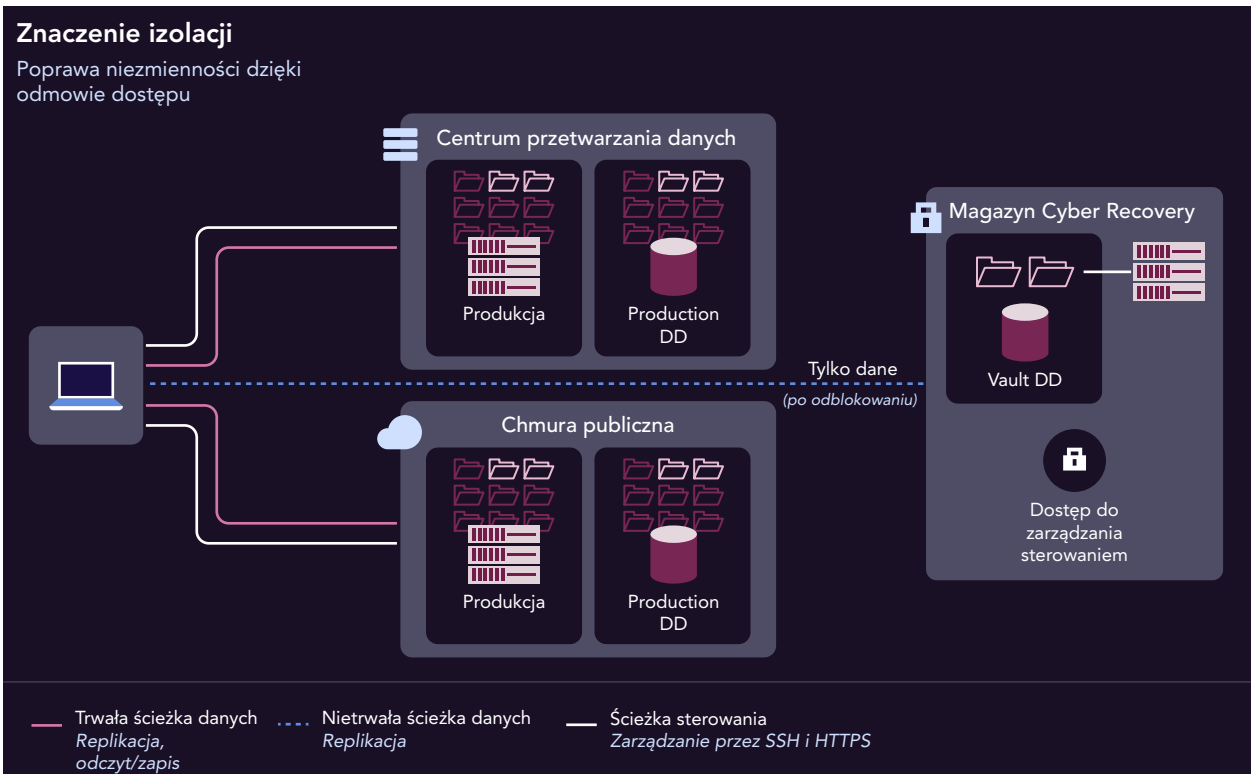
Przeglądając publicznie dostępne informacje na temat rozwiązań Cohesity, Veeam, Rubrik i Veritas, stwierdziliśmy, że każde z nich ma co najmniej nieco inne podejście do IRE od PowerProtect Cyber Recovery. Dzięki rozwiązaniu firmy Dell klienci mogą fizycznie lub logicznie odizolować swoje sejfy DD od produkcji, aby utrzymać płaszczyzny sterowania i danych produkcji z dala od sejfów. Ponadto rozwiązanie PowerProtect Cyber Recovery automatyzuje izolacje, co nie wszystkie inne rozwiązania robią.

Zgodnie z dokumentacją:

- Cohesity Cyber Recovery oferuje tylko dynamiczną zautomatyzowaną izolację logiczną sejfu FortKnox opartego na AWS.[19]
- Veeam obsługuje izolację logiczną dla dostawców chmury publicznej i prywatnej poprzez Veeam Cloud Connect, ale bez automatyzacji. Firma Veeam oferuje również zabezpieczone repozytorium Veeam, które działa jako sejf lokalny dla rozwiązania i które organizacje mogą skonfigurować w celu uzyskania fizycznej izolacji.[20]
- Rubrik nie oferuje zautomatyzowanej izolacji sejfu Rubrik w chmurze, ale klienci mogą dodać izolację logiczną poprzez zewnętrzną współpracę z firmą Microsoft.[21]
- Klienci NetBackup muszą ręcznie włączyć izolację logiczną i mogą utworzyć izolację fizyczną za pomocą rozwiązania lokalnego lub zewnętrznego.[22]

Zasada działania

Rysunek 1 przedstawia ścieżki sieciowe odizolowanego sejfu Cyber Recovery. Należy pamiętać, że sejf nie ma ścieżki zarządzania ani kontroli do środowiska produkcyjnego, co ogranicza płaszczyznę ataku.



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

Jedynym wymaganym połączeniem dla sejfu Cyber Recovery jest ścieżka danych do okresowej synchronizacji danych. Synchronizacja polega na tym, że rozwiązanie Cyber Recovery pobiera dane w krótkich, opartych na regułach interwałach na potrzeby replikacji.[23] Podręcznik rozwiązania PowerProtect Cyber Recovery stwierdza, że „architektura rozwiązania Cyber Recovery na poziomie podstawowym składa się z pary systemów PowerProtect DD i hosta zarządzania Cyber Recovery. W tej konfiguracji na poziomie podstawowym oprogramowanie Cyber Recovery, które działa na hoście zarządzającym, włącza i wyłącza interfejs replikacji Ethernet wraz z kontekstami replikacji w systemie PowerProtect DD w sejfie Cyber Recovery w celu kontrolowania przepływu danych ze środowiska produkcyjnego do środowiska sejfu”.[24] Firma Dell sugeruje dodatkowe sposoby zabezpieczania i izolowania ścieżek danych. Podczas naszych testów zaobserwowaliśmy odblokowanie i blokowanie sejfu Cyber Recovery podczas replikacji i po jej zakończeniu.

Dla potrzeb fizycznej implementacji sejfu firma Dell zaleca „zainstalowanie sprzętu sejfu Cyber Recovery w specjalnym pomieszczeniu lub klatce z fizyczną kontrolą dostępu”. To zabezpieczone pomieszczenie powinno mieć ograniczoną listę dostępu z wylogowaniem przy użyciu klucza lub dostępem za pomocą kluczy dwóch osób. Należy zapewnić nadzór wideo punktów wejścia do klatki lub pomieszczenia oraz sprzętu. Aby zapewnić maksymalne bezpieczeństwo, oprogramowanie Cyber Recovery musi być dostępne tylko poprzez fizyczny dostęp do serwera zarządzania Cyber Recovery oraz powiązanej klawiatury i myszy”.[25]

Dzięki oddzieleniu ścieżek zarządzania i kontroli opcje izolacji fizycznej i logicznej Cyber Recovery wyróżniają się na tle innych rozwiązań. Niektóre rozwiązania umożliwiają dostęp do danych sejfu z poziomu interfejsu środowiska produkcyjnego. Powoduje to umieszczenie danych sejfu na tej samej powierzchni ataku, co dane produkcyjne, co może pozwolić złośliwym podmiotom na dostęp do kopii zapasowych za pomocą naruszonych danych uwierzytelniających.

CyberSense

Skuteczna ochrona danych wymaga kompleksowej strategii, która zapewnia bezpieczeństwo na każdym poziomie. Pomimo wszystkich mechanizmów autonaprawy, zabezpieczeń, niezmienności i funkcji izolacji, jakie udostępnia rozwiązanie Dell PowerProtect Cyber Recovery, mniej oczywiste ataki mogłyby nadal wnikać głębiej w infrastrukturę przedsiębiorstwa, np. na poziom zapasowych kopii danych, i potencjalnie pozostawać niewykryte do czasu naruszenia bezpieczeństwa danych produkcyjnych lub całej grupy użytkowników. Rozwiązania Dell PowerProtect Cyber Recovery stanowią ostatnią linię obrony przed cyberatakami i skuteczny środek przyspieszający odzyskiwanie danych dzięki funkcji CyberSense. CyberSense to mechanizm analityczny, który wykorzystuje algorytmy analizy ML oparte na sztucznej inteligencji do skanowania i weryfikacji integralności kopii zapasowych w sejfie oraz zawartości użytkownika plików w kopiach zapasowych.

CyberSense działa wewnątrz sejfu, odizolowanego od środowiska produkcyjnego. Śledzi pliki, obrazy maszyn wirtualnych i bazy danych wewnątrz sejfu, aby ustalić, czy doszło do ataku, analizując integralność danych. Gdy rozwiązanie Cyber Recovery replikuje kopie zapasowe do sejfu i stosuje funkcję Retention Lock, rozwiązanie CyberSense automatycznie skanuje kopie i tworzy obrazy plików, baz danych i podstawowej infrastruktury z punktu w czasie. Silnik analityczny skanuje pełną zawartość plików i każdej strony bazy danych — nie tylko metadane. Gdy inne rozwiązania szukają zmian w progach danych lub metadanych, CyberSense sprawdza zawartość plików w celu sprawdzenia integralności danych. Obserwacje te pozwalają CyberSense śledzić, jak pliki i bazy danych zmieniają się w czasie i odkryć wiele zaawansowanych rodzajów ukrytych ataków. Następnie CyberSense generuje analizy, które wykrywają wzorce uszkodzeń, które mogą wskazywać na aktywność złośliwego podmiotu, w tym szyfrowanie, usuwanie, tworzenie lub zaciemnianie plików i nie tylko.[26] Inne rozwiązania przenoszą analizę do chmury, co może rozszerzyć powierzchnię ataku, a organizacje mogą uruchomić CyberSense lokalnie lub w jednej z wielu opcji chmury obsługiwanych przez Cyber Recovery.

CyberSense łączy w sobie ponad 200 analiz z obserwacjami danych, które stają się coraz bardziej przydatne w miarę wzrostu liczby obserwacji. Algorytm ML wykorzystuje informacje o tysiącach infekcji złośliwym oprogramowaniem, aby znaleźć nietypowe wzorce zachowań i odróżnić aktywność użytkowników od ransomware, a jednocześnie ograniczyć do minimum wyniki fałszywie pozytywne i negatywne. Algorytm otrzymuje nową wiedzę na temat takich kwestii, jak warianty ataków, dzięki ciągłym badaniom. Ponadto algorytm ML otrzymuje aktualizacje na podstawie rzeczywistych danych od istniejących klientów CyberSense.[27]

Ponadto CyberSense obsługuje indeksowanie danych w popularnych formatach dyskowych kopii zapasowych firm Dell, IBM, Commvault i Veritas.[28] Poprzez wspieranie formatów kopii zapasowych od innych dostawców, firma Dell pokazuje gotowość do spotkań z klientami w zakresie tworzenia kopii zapasowych danych.

Przetestowaliśmy oprogramowanie do inteligentnej analizy oparte na uczeniu maszynowym dwóch gotowych do użycia cyber rozwiązań ochrony i odzyskiwania danych dla przedsiębiorstw: CyberSense for Dell PowerProtect Cyber Recovery na serwerze Dell PowerStore™ 7000T oraz podobnie działające narzędzie z platformy zarządzania danymi konkurenta („Dostawca X") przeznaczone do urządzenia o podobnej wielkości.

Sposób testowania

Przeprowadziliśmy wszystkie testy zdalnie i mieliśmy pełną kontrolę nad testami oraz nieskrępowany dostęp do nich. Zarówno rozwiązanie firmy Dell (w tym CyberSense, aplikacja do tworzenia kopii zapasowych PowerProtect Data Manager, APEX Protection Storage (wcześniej DD Virtual Edition), jak i rozwiązanie PowerProtect Cyber Recovery) oraz rozwiązanie Dostawcy X znajdowały się w laboratorium zewnętrznego centrum przetwarzania danych.

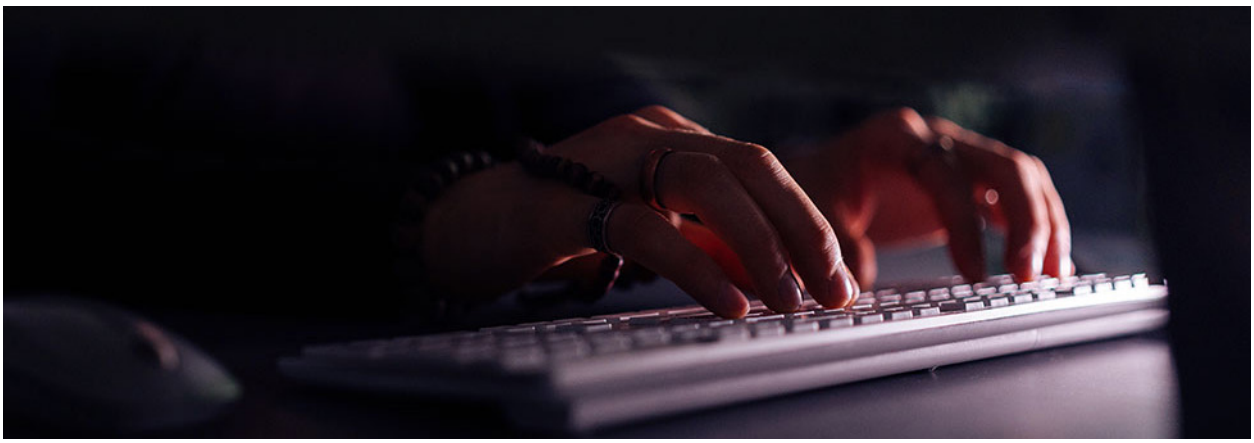
W obu rozwiązaniach uruchomiliśmy trzy scenariusze złośliwych zdarzeń oparte na skryptach, które ukierunkowały kopie zapasowe:

Rysunek 2: Nasze scenariusze testowe. Źródło: Principled Technologies.

W przypadku obu rozwiązań pierwsze dwa scenariusze przebiegały zgodnie z tą samą ogólną procedurą. Najpierw utworzyliśmy pełną kopię zapasową wszystkich czystych maszyn wirtualnych na urządzeniach pamięci masowej Dell PowerProtect Data Manager i Dostawcy X, utworzyliśmy przyrostowe kopie zapasowe do skanowania i sprawdziliśmy, czy rozwiązanie docelowe nie wykryło zagrożenia. Dało nam to podstawowy zestaw kopii zapasowych, na których mogliśmy wykonać skrypty ataku.

Następnie wykonaliśmy skrypt symulacji ransomware na czterech maszynach wirtualnych z różnymi systemami operacyjnymi i typami aplikacji, wykonaliśmy nowe przyrostowe kopie zapasowe na urządzeniu docelowym i sprawdziliśmy, czy docelowe oprogramowanie analityczne wykryje zagrożenie szyfrowania.

W przypadku trzeciego scenariusza (Infekcja strony serwera SQL) zastosowaliśmy procedurę podobną jak w dwóch innych scenariuszach, ale zamiast tego skupiliśmy się na maszynach wirtualnych SQL i użyliśmy skryptu uszkodzenia strony, a nie skryptu szyfrowania. Skrypt został uruchomiony na jednej maszynie wirtualnej.



Co odkryliśmy

Scenariusz 1: Wykrywanie zaszyfrowanych plików z zaciemnionymi nazwami plików

Ten scenariusz symulował złośliwe zdarzenie, które szyfrowało pliki i zaciemniało ich nazwy, co zmieniło metadane pliku oprócz jego zawartości. Ten typ ataku jest zwykle znany jako ransomware, zdarzenie bezpieczeństwa, w którym złośliwe oprogramowanie blokuje dostęp do systemu komputerowego do chwili, gdy właściciel lub użytkownik systemu zapłaci wstępnie określoną kwotę pieniędzy. Według amerykańskiej organizacji Cybersecurity and Infrastructure Security Agency (CISA) „skutki ekonomiczne i wizerunkowe ransomware i wymuszeń danych okazały się trudne i kosztowne dla organizacji każdej wielkości podczas początkowych zakłóceń, a czasami także dłuższego odzyskiwania”.[29] Korzystanie z oprogramowania do inteligentnej analizy w celu wykrywania szyfrowania w kopiach zapasowych może wzmocnić strategię ochrony danych każdej organizacji, pomóc w zabezpieczaniu cennych i poufnych informacji oraz zmniejszyć ryzyko kosztownych przestojów spowodowanych cyberatakami.

W naszych testach obie inteligentne aplikacje analityczne wykryły zaszyfrowane pliki ze zmienionymi nazwami plików. Rozwiązanie Dostawcy X wymagało podstawowej liczby 15 kopii zapasowych, zanim wykryło infekcje (jedna pełna kopia zapasowa i 14 przyrostowe kopie zapasowe), podczas gdy CyberSense wykrył infekcje po zaledwie jednej pełnej kopii zapasowej, co oznacza, że rozwiązanie Dostawcy X wymagało 14 dodatkowych kopii zapasowych w porównaniu z CyberSense.

Gdy rozwiązanie Dostawcy X powiadomiło nas o podejrzanej aktywności, wskazało tylko, że coś usunęło wiele plików i dodało taką samą liczbę plików, co było podejrzaną aktywnością na podstawie oceny entropii kopii zapasowej.[30] Rozwiązanie Dostawcy X nie wykazało, że pliki zostały zaszyfrowane ani że nazwy plików uległy zmianie. Z kolei rozwiązanie Cyber Recovery z CyberSense zaalarmowało nas, że coś zaszyfrowało i zaciemniło nazwy plików.

Wyniki dla Dostawcy X mogą wskazywać fałszywie pozytywny wynik. Innymi słowy, jeśli założymy, że organizacja wykonuje codzienne kopie zapasowe przy użyciu rozwiązania Dostawcy X, mogła ona przyswajać zainfekowane pliki przez 14 dni przed wykryciem anomalii. Z kolei rozwiązanie CyberSense potrzebowało tylko jednej bazowej kopii do inteligentnego ostrzegania o infekcji i jej szczegółach. W naszym przykładzie odzyskiwanie za pomocą rozwiązania Cyber Recovery odbywa się z izolowanego sejfu, co gwarantuje organizacji, że sieć produkcyjna nie będzie narażona na 14 zainfekowanych kopii zapasowych, co byłoby możliwe w przypadku rozwiązania Dostawcy X.

Rysunek 3: Liczba kopii zapasowych wymaganych przez każde rozwiązanie do utworzenia wartości początkowej w celu wykrycia uszkodzenia.
Źródło: Principled Technologies.

Scenariusz 2: Wykrywanie zaszyfrowanych plików z oryginalnymi nazwami plików

Ten scenariusz był podobny do pierwszego scenariusza, ale skrypt zachował oryginalne nazwy plików zaszyfrowanych plików. Ta zmiana nie wpłynęła na metadane plików, tylko na same pliki. Takie działanie może okazać się ransomware z opóźnionym zapłonem, w którym atak pozostaje uśpiony przez pewien czas przed aktywacją. Ransomware z opóźnionym zapłonem może uniknąć wykrycia i zaatakować kopie zapasowe, przez co zainfekowane kopie zapasowe staną się bezużyteczne, gdy organizacja będzie ich potrzebować.[31] Bez zmian w metadanych plik może wydawać się niezainfekowany na powierzchni, co pomaga utrzymać uśpiony atak w ukryciu.

W naszych testach obie inteligentne aplikacje analityczne wykryły zaszyfrowane pliki. Ponownie rozwiązanie Dostawcy X wymagało podstawowej liczby 15 kopii zapasowych, w tym 14 przyrostowych kopii zapasowych, zanim wykryje anomalię. Rozwiązanie CyberSense potrzebowało tylko jednej bazowej pełnej kopii zapasowej do wykrycia anomalii.

Podobnie jak w pierwszym scenariuszu, rozwiązanie Dostawcy X zaalarmowało nas tylko, że coś zmieniło wiele plików, co było podejrzane w oparciu o ocenę entropii kopii zapasowej. Nie wskazało, że coś zaszyfrowało pliki, podczas gdy rozwiązanie Cyber Recovery z CyberSense nam o tym poinformowało. Wykrywanie uszkodzeń w ten sposób oznacza, że CyberSense analizuje zawartość plików, a nie tylko metadane na poziomie powierzchni. Ten rodzaj skanowania dodaje kolejną warstwę bezpieczeństwa dla twoich kopii zapasowych, a tym samym dla twojej cyfrowej infrastruktury lub majątku w ogóle. Można sugerować, że CyberSense jest „prawdziwą" inteligentną aplikacją analityczną. Ponadto organizacje mogą szybciej wykrywać uszkodzenia dzięki CyberSense, ponieważ rozwiązanie wymaga znacznie mniejszej liczby kopii zapasowych do utworzenia wartości początkowej. W zależności od harmonogramu tworzenia kopii zapasowych organizacji może to nastąpić wiele dni wcześniej.

Rysunek 4: Liczba kopii zapasowych każdego rozwiązania wymaganego do wykrycia uszkodzenia. Źródło: Principled Technologies.

Scenariusz 3: Wykrywanie uszkodzenia strony SQL Server

Ten scenariusz symulował złośliwe zdarzenie, które powoduje uszkodzenie strony SQL Server. W przypadku serwera SQL Server podstawową jednostką przechowywania danych jest strona, a baza danych odczytuje lub zapisuje całe strony danych.[32] Ponownie, ta zmiana nie wpłynęła na metadane, tylko na same pliki. Ten typ ataku jest powszechnie znany jako iniekcja SQL, w której atakujący atakują aplikacje oparte na danych SQL poprzez wprowadzanie złośliwego kodu do instrukcji SQL za pośrednictwem strony internetowej.[33] Nawet w przypadku zainfekowania bazy danych mogą nadal działać. Oprócz kradzieży danych uszkodzenie stron programu SQL Server może spowodować problemy z integralnością danych, utratę danych i zakłócenia funkcjonalności bazy danych. Te wyniki mogą uszkodzić reputację organizacji, zakłócić przepływy pracy operacyjne, spowodować straty finansowe, a nawet spowodować odpowiedzialność prawną.

Chociaż rozwiązania CyberSense i Dostawcy X wykryły szyfrowanie w pierwszych dwóch scenariuszach, tylko CyberSense był w stanie skanować wystarczająco głęboko, aby wykryć uszkodzenie na stronie SQL Server w tym trzecim scenariuszu. Pokazuje to, że chociaż te dwa rozwiązania oferują podobne możliwości wykrywania na niektórych poziomach, CyberSense oferuje głębsze skanowanie kopii zapasowych potencjalnie krytycznych dla działalności aplikacji opartych na SQL Server. W ten sposób CyberSense dodaje warstwę odporności na zagrożenia dzięki głębszemu skanowaniu i bardziej kompleksowej ochronie.

SQL Server obsługuje wiele aplikacji w branżach finansowych, handlu detalicznego, opieki zdrowotnej i innych. Ponieważ SQL Server może działać jako zaplecze architektury deweloperskiej, atak SQL Server może spowodować przestoje, przerwanie operacji i potencjalnie zagrozić przychodowi generowanemu przez te aplikacje.

Przywracanie i odzyskiwanie danych dzięki rozwiązaniu Dell PowerProtect Cyber Recovery

Strategia cyberodporności firmy Dell zapewnia szeroki zakres możliwości odzyskiwania danych. Te opcje odzyskiwania obejmują typowe funkcje branżowe, takie jak natychmiastowy dostęp lub tradycyjne odzyskiwanie z niezmiennych kopii zapasowych utrzymywanych w produkcji. Ponadto firma Dell zapewnia wyjątkowe możliwości odzyskiwania danych dzięki rozwiązaniu PowerProtect Cyber Recovery. Ponieważ rozwiązanie PowerProtect Cyber Recovery utrzymuje kopie w izolacji i skanuje je pod kątem integralności za pomocą CyberSense, organizacje mogą uzyskać dostęp do kopii natychmiast po ataku i użyć ich do rozpoczęcia czynności odzyskiwania lub natychmiastowego przywrócenia do alternatywnych platform odzyskiwania, takich jak pomieszczenia czyste.

Porównaj ten przypadek natychmiastowego użycia z organizacją, która może uzyskać dostęp tylko do danych w produkcji lub chmurze publicznej. Organizacja nie może bezpiecznie uzyskać dostępu do danych przechowywanych w naruszonym obszarze do czasu ustalenia i naprawienia przyczyny źródłowej, wykluczenia złośliwych podmiotów, wykonania obrazów śledczych dla potrzeb ubezpieczycieli i działu prawnego, ponownego przeskanowania danych i posiadania wystarczającej infrastruktury (AD, DNS) do uzyskiwania dostępu do infrastruktury kopii zapasowych. Proces ten może potrwać kilka dni lub tygodni w zależności od zakresu i zaawansowania ataku.

Zasada działania

Podczas normalnej produkcji PowerProtect Cyber Recovery automatycznie tworzy punkty przywracania do odzyskiwania i analizy zabezpieczeń. W przypadku cyberataku Cyber Recovery wykorzystuje swoje zautomatyzowane procedury przywracania i odzyskiwania oraz punkty przywracania, aby przywrócić systemy o znaczeniu krytycznym dla firmy. CyberSense i raporty z badań pomagają zespołom cyberbezpieczeństwa i odzyskiwania danych zdiagnozować wpływ ataku. Gdy środowisko produkcyjne będzie czyste i gotowe do odzyskania, Cyber Recovery zapewnia narzędzia i technologię, które umożliwiają rzeczywiste odzyskiwanie danych.

Po cyberataku istnieje wiele wskaźników ochrony danych, które determinują szybkość odzyskiwania (czas cyberpowrotu do stanu normalnego lub CRT) i punkt w czasie, do którego mogą wrócić użytkownicy po niszczącym ataku (punkt odzyskiwania lub CRP). W przypadku rozwiązania Cyber Recovery wskaźniki te obejmują następujące elementy:

- **Cel wykrywania zniszczeń (DDO):** To jest okno kroczące oparte na ilości czasu od ataku do wykrycia ataku. Analityka i inne mechanizmy odzyskiwania cybernetycznego muszą działać w tym okresie.
- **Cel oceny niszczenia (DAO):** Jest to czas przydzielony zespołowi ds. cyberbezpieczeństwa po naruszeniu zabezpieczeń w celu określenia zakresu uszkodzeń i potencjalnych reakcji.
- **Interwał synchronizacji Cyber Recovery:** Jest to częstotliwość, z jaką rozwiązanie Cyber Recovery kopiuje dane ze środowiska produkcyjnego do sejfu. Czas jest oparty na wcześniej ustalonym celu punktu odzyskiwania (RPO) dla rozwiązania. Okres przechowywania kopii różni się w zależności od rozwiązania, ale zazwyczaj wynosi od tygodnia do miesiąca.
- **Liczba kopii danych Cyber Recovery:** Jest to liczba kopii danych przechowywanych w sejfie Cyber Recovery. W połączeniu z interwałem synchronizacji wskaźnik ten stanowi zgrubną miarę odległości w czasie, z jakiej organizacja może odzyskać dane, np. siedem kopii w połączeniu z interwałem 24-godzinnym pozwala użytkownikom odzyskać dane w wieku do jednego tygodnia.

Oprócz wymagań dotyczących odzyskiwania, typ danych, które chroni rozwiązanie, może pomóc w określeniu interwału synchronizacji danych i czasu przechowywania. Zgodnie z przewodnikiem po rozwiązaniach Cyber Recovery, aby uzyskać największą elastyczność odzyskiwania, użytkownicy mogą kategoryzować dane, które rozwiązanie chroni, w jednym z następujących strumieni kopii zapasowych:[34]

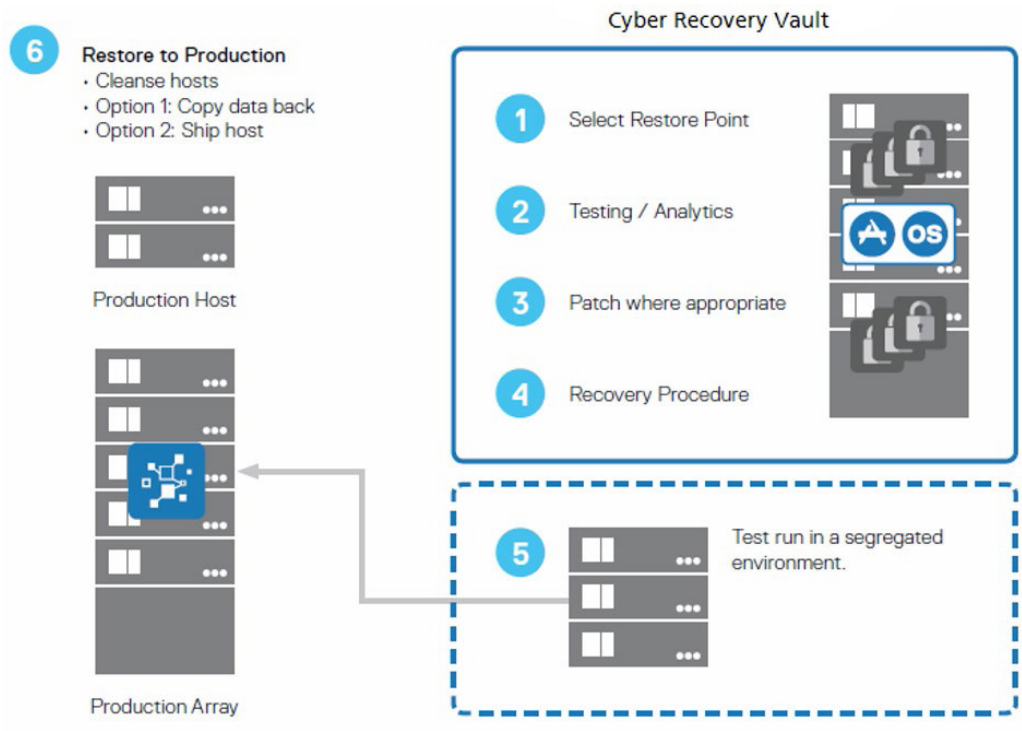
- Kopie zapasowe binarne i wykonywalne, w tym dystrybucje systemów operacyjnych na poziomie

podstawowym i kompilacje aplikacji

- Pełne kopie zapasowe aplikacji i systemów plików, w tym obrazy i dane specyficzne dla aplikacji

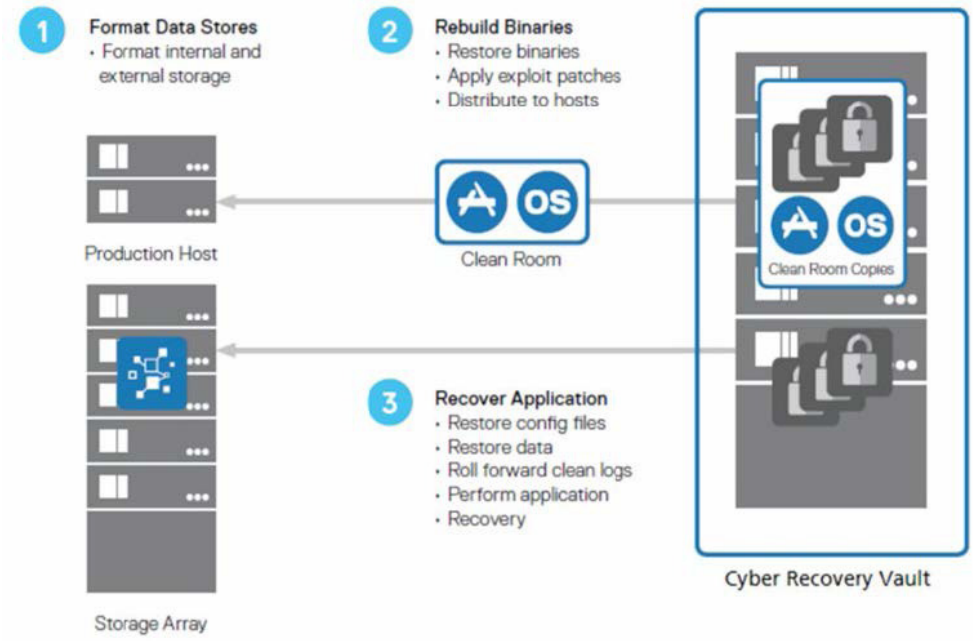
Te oddzielne strumienie kopii zapasowych prowadzą do dwóch różnych strategii odzyskiwania:

1. **Przywracanie plików binarnych danych i aplikacji w sejfie Cyber Recovery:**
   Rozwiązanie identyfikuje przydatne punkty przywracania, a także złośliwe oprogramowanie i to, gdzie się utrzymało, a następnie decyduje, czy oczyścić złośliwe oprogramowanie z kopii zapasowej obrazu lub odbudować przy użyciu kopii zapasowych Cyber Recovery z sejfu. Po zastosowaniu poprawek zabezpieczeń rozwiązanie przywraca dane do hosta odzyskiwania przy użyciu instrukcji DR dla aplikacji, a następnie określa, czy proces odzyskiwania wyeliminował skutki złośliwego oprogramowania. Następnie przeprowadza uruchomienie testowe aplikacji przy użyciu zasobów obliczeniowych sejfu i oczyszcza lub ponownie tworzy obrazy środowiska produkcyjnego. Na koniec Cyber Recovery łączy hosta odzyskiwania z produkcją i kopiuje aplikację i dane z powrotem do środowiska produkcyjnego. Rysunek 5 przedstawia ten proces.



Rysunek 5: Proces przywracania plików binarnych danych i aplikacji. Źródło: Dell Technologies.[35]

2. **Całkowita przebudowa z sejfu Cyber Recovery:**
   W tym podejściu rozwiązanie Cyber Recovery reformatuje systemy produkcyjne w oparciu o poziom uszkodzeń określony przez ocenę śledczą podczas reagowania na incydenty. Rozwiązanie odbudowuje pliki binarne za pomocą kopii w sejfie Cyber Recovery i stosuje dostępne poprawki zabezpieczeń. Na koniec przywraca odpowiednie kopie aplikacji, danych i plików konfiguracyjnych do środowiska produkcyjnego przy użyciu powiązanych katalogów DR dla aplikacji. Rysunek 6 przedstawia ten proces.



Rysunek 6: Proces całkowitej odbudowy z sejfu Cyber Recovery. Źródło: Dell Technologies.[36]

Rozwiązania Cyber Recovery obejmują fizyczne lub wirtualne hosty odzyskiwania (lub oba), które oprogramowanie Cyber Recovery może wykorzystywać do odzyskiwania. Hosty te obejmują zarówno serwer aplikacji odzyskiwania kopii zapasowych, który jest specjalnym serwerem, na którym aplikacja do tworzenia kopii zapasowych kataloguje kopie zapasowe, oraz serwer aplikacji odzyskiwania. Organizacje mogą wdrożyć wiele serwerów w zależności od wymagań rozwiązania dotyczących odzyskiwania. Oprogramowanie Cyber Recovery może udostępniać kopie danych typu sandbox (środowisko testowe do bezpiecznego uruchamiania nowego lub nieprzetestowanego oprogramowania) każdemu hostowi w celu wykonania odzyskiwania danych w sejfie, takich jak dane systemu plików, dane kopii zapasowych IBM, Commvault i Veritas bądź dane chronione przez Dell NetWorker, Dell Avamar, urządzenie Dell PowerProtect serii DP lub oprogramowanie Dell PowerProtect Data Manager. Po odzyskaniu aplikacji do tworzenia kopii zapasowych w sejfie rozwiązanie może przywrócić te dane do dodatkowych hostów odzyskiwania w sejfie.

Organizacje z wyprzedzeniem skalują serwer odzyskiwania aplikacji do tworzenia kopii zapasowych, aby użytkownicy mogli odzyskać wszystkie aplikacje do tworzenia kopii zapasowych, które chroni rozwiązanie Cyber Recovery. Podobnie serwer odzyskiwania aplikacji jest wyznaczonym serwerem, na którym rozwiązanie odzyskuje aplikacje. Niektóre aplikacje mogą wymagać od klientów przywrócenia najpierw innych zależnych aplikacji. Infrastruktura w sejfie może obsługiwać odzyskiwanie największej aplikacji produkcyjnej, którą chroni rozwiązanie.

Wnioski

Organizacje muszą wziąć pod uwagę wiele wektorów ataków podczas tworzenia planu ochrony danych. Obejmuje to ochronę wszystkich danych, ale przede wszystkim danych o znaczeniu krytycznym dla operacji. Rozwiązanie PowerProtect Cyber Recovery izoluje dane o znaczeniu krytycznym i pomaga zapewnić prawidłowe odzyskiwanie danych w przypadku cyberataku. Cyber Recovery wykorzystuje analitykę opartą na uczeniu maszynowym w silniku CyberSense w celu określenia integralności danych w sejfie i identyfikowania czystych danych kopii zapasowych do odzyskania. Z naszych testów wynika, że rozwiązanie PowerProtect Cyber Recovery wykryło zarażenie na stronach bazy danych SQL — rozwiązanie konkurencyjne nie było w stanie tego zrobić. PowerProtect Cyber Recovery wymagało też mniejszej liczby kopii zapasowych niż rozwiązanie konkurencyjne w celu wykrycia uszkodzenia danych. Oprócz tego wszystkiego i nie tylko rozwiązanie Cyber Recovery zapewnia wiele opcji odtwarzania po awarii, polegając na nienaruszonych danych z sejfu dla wydajnego i płynnego powrotu do pracy.

---

1. Dell, „CyberSense® for PowerProtect Cyber Recovery", dostęp: 8 września 2023 r., https://www.delltechnologies.com/asset/en-in/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
2. Dell, „Dell PowerProtect Cyber Recovery Solution Guide", dostęp: 23 sierpnia 2023 r., https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
3. Dell, „Dell PowerProtect Cyber Recovery Solution Guide".
4. Cohasset Associates, Inc, „Dell Technologies PowerProtect DD and DDVE – Compliance Assessment: SEC 17a-4(f), SEC 18a-6(e) and FINRA 4511(c)", dostęp: 27 października 2023 r., https://infohub.delltechnologies.com/section-assets/cohasset-dell-powerprotect-dd-compliance-assessment.
5. Dell, „Data Domain: Retention Lock Frequently Asked Questions", dostęp: 12 września 2023 r., https://www.dell.com/support/kbdoc/en-us/000079803/data-domain-retention-lock-frequently-asked-questions-faq.
6. Dell, „Data Domain: Retention Lock – najczęściej zadawane pytania".
7. Dell, „Encryption types offered by DD series encryption appliance", dostęp: 8 września 2023 r., https://infohub.delltechnologies.com/l/powerprotect-dd-series-appliances-encryption-software-1/encryption-types-offered-by-dd-series-encryption-appliance.
8. Dell, „Dell EMC Data Domain – Security Configuration Guide", dostęp: 11 września 2023 r., https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu91808.pdf.
9. Dell, „Role based access control (RBAC) in Data Domain", dostęp: 11 września 2023 r., https://www.dell.com/community/en/conversations/data-domain/role-based-access-control-rbac-in-data-domain/647f70a9f4ccf8a8dee30f99.
10. Dell, „Dell EMC Data Domain — podręcznik konfiguracji zabezpieczeń".
11. Dell, „MTree replication" (Replikacja MTree), dostęp 11 września 2023 r., https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3.

12. Veeam, „Dell EMC Data Domain - DataDomain MTree overview and limits", dostęp: 11 września 2023 r., https://bp.veeam.com/vbr/2_Design_Structures/D_Veeam_Components/D_backup_repositories/datadomain.html
13. Chris Wahl, „Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture", dostęp 13 grudnia 2023 r., https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
14. Veritas, „NetBackup™ Security and Encryption Guid", dostęp: 13 grudnia 2023 r., https://www.veritas.com/support/en_US/doc/21733320-149123528-0/v143394540-149123528.
15. Principled Technologies, „Dell EMC Cyber Recovery protected our test data from a cyberattack" (Rozwiązanie Dell EMC Cyber Recovery ochroniło nasze dane testowe przed cyberatakiem), dostęp 21 sierpnia 2023 r., http://facts.pt/rkew01n.
16. Dell, „Dell PowerProtect Cyber Recovery", dostęp: 12 września 2023 r., https://www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/isolated-recovery-solution-overview.pdf.
17. Jerry Rozeman i Michael Hoeck, „Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware", dostęp: 14 grudnia 2023 r., https://www.gartner.com/doc/reprints?id=1-27MOHCBD&ct=211011&st=sb.
18. Jerry Rozeman i Michael Hoeck, „Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware".
19. Nikitha Okmar, „Going Beyond the Air Gap - Data Isolation and Recovery for the Modern Era", dostęp: 13 grudnia 2023 r., https://www.cohesity.com/blogs/going-beyond-the-air-gap-data-isolation-and-recovery-for-the-modern-era/.
20. Marco Horstmann, „How to protect your data from ransomware and encryption Trojans", dostęp: 13 grudnia 2023 r., https://www.veeam.com/blog/how-to-protect-against-ransomware-data-loss-and-encryption-trojans.html.
21. Rubrik, „Rest easy with immutable, off-site data storage", dostęp: 13 grudnia 2023 r., https://www.rubrik.com/products/rubrik-cloud-vault.
22. Veritas, „NetBackup Isolated Recovery Environment", dostęp: 13 grudnia 2023 r., https://www.veritas.com/content/dam/www/en_us/documents/solution-overview/SO_flex_appliance_netbackup_ire_solution_V1543.pdf.
23. CSI Group, „Dell Cyber Recovery Vault (overview by CSI)", dostęp: 23 sierpnia 2023 r., https://youtu.be/ej5nZzWNRM0.
24. Dell, „Przewodnik po rozwiązaniu Dell PowerProtect Cyber Recovery".
25. Dell, „Przewodnik po rozwiązaniu Dell PowerProtect Cyber Recovery".
26. Dell, „CyberSense® for PowerProtect Cyber Recovery".
27. Dell, „CyberSense® for Dell PowerProtect Cyber Recovery – Powered by Index Engines", dostęp: 13 września 2023 r., https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/cybersense-for-dell-powerprotect-cyber-recovery-whitepaper.pdf.
28. Index Engines, „CyberSense for Dell Cyber Recovery", dostęp: 25 września 2023 r., https://indexengines.com/csmatrix.
29. CISA, „#StopRansomware Guide", dostęp: 1 sierpnia 2023 r., https://www.cisa.gov/stopransomware/ransomware-guide.
30. „W zakresie bezpieczeństwa większość ludzi używa entropii Shannona — określonego algorytmu, który zwraca wartość od 0 do 8. Im wyższa liczba, tym bardziej losowe dane, a często wyższa wartość oznacza, że dane są spakowane lub zaszyfrowane". Mueller, Clint, „How to Use Entropy Analysis in Penetration Testing", 28 sierpnia 2023 r., https://www.schellman.com/blog/cybersecurity/penetration-testing-methods-entropy.
31. Cooper, Steven, „How to Protect your Backups from Ransomware in 2023", 1 sierpnia 2023 r., https://www.comparitech.com/net-admin/protect-backups-from-ransomware/.
32. Microsoft, „Pages and extents architecture guide", dostęp: 3 sierpnia 2023 r., https://learn.microsoft.com/en-us/sql/relational-databases/pages-and-extents-architecture-guide?view=sql-server-ver16.
33. W3 Schools, „SQL Injection", dostęp 3 sierpnia 2023 r., https://www.w3schools.com/sql/sql_injection.asp.
34. Dell, „Przewodnik po rozwiązaniu Dell PowerProtect Cyber Recovery".
35. Dell, „Przewodnik po rozwiązaniu Dell PowerProtect Cyber Recovery".
36. Dell, „Przewodnik po rozwiązaniu Dell PowerProtect Cyber Recovery".

Przeczytaj informacje naukowe zawarte w tym raporcie ▶

▶ Zobacz oryginalną, angielską wersję tego raportu na stronie https://facts.pt/64FU3b2

Principled Technologies®

Facts matter.®

Projekt ten został zlecony przez Dell Technologies.