DELL Technologies

Krótki opis rozwiązania

Dell PowerProtect Cyber Recovery

Nowoczesna i odporna ochrona danych o znaczeniu krytycznym przed ransomware i destrukcyjnymi cyberatakami.

DLACZEGO WARTO KORZYSTAĆ Z CYBER RECOVERY?

Cyberataki mają na celu naruszenie cennych danych, w tym kopii zapasowych. Ochrona najważniejszych danych i odzyskanie ich z gwarancją integralności jest kluczem do wznowienia normalnej działalności po ataku.

Poniżej przedstawiono elementy składowe rozwiązania odpornego na cyberataki:

Niezmienność danych
Twórz niezmienne kopie danych, aby zachować integralność i poufność danych dzięki warstwom zabezpieczeń i kontroli.

Izolacja danych i zarządzanie nimi
Izolowane środowisko odzyskiwania danych odłączone od sieci firmowych i sieci kopii zapasowych z podwyższonym poziomem ograniczeń dostępu użytkowników.

Automatyczne kopiowanie danych i fizyczna izolacja
Twórz niezmienne kopie danych w bezpiecznym magazynie cyfrowym i procesach, które tworzą fizyczną izolację między środowiskiem produkcji / kopii zapasowych a magazynem.

Inteligentna analiza
Zautomatyzowane sprawdzanie integralności przy użyciu opartych na sztucznej inteligencji mechanizmów uczenia maszynowego i indeksowanie całej zawartości z zaawansowaną analizą w ramach bezpieczeństwa magazynu w celu określenia, czy dane zostały naruszone przez złośliwe oprogramowanie.

Odzyskiwanie i działania zaradcze
Przepływy pracy i narzędzia do odzyskiwania danych po incydentach przy użyciu procesów dynamicznego przywracania i istniejących procedur DR.

Planowanie i projektowanie rozwiązań
Specjalistyczne wskazówki dotyczące wyboru najważniejszych zestawów danych, aplikacji i innych ważnych zasobów w celu określenia wartości RTO i RPO oraz usprawnienia odzyskiwania.

Wyzwanie: cyberataki są wrogiem firm opartych na danych.

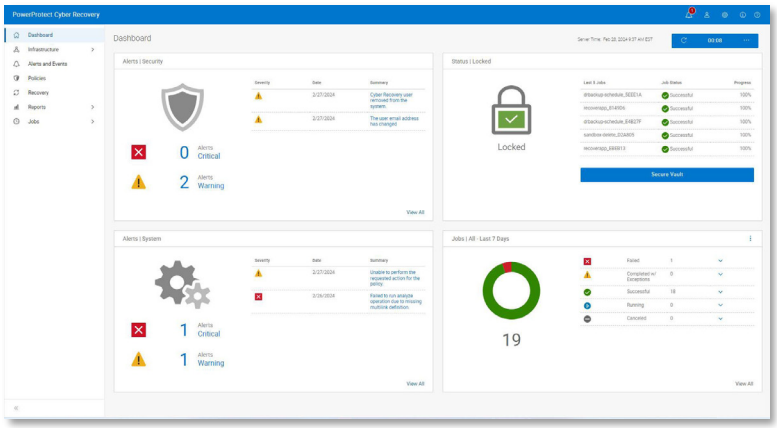
Dane to waluta gospodarki cyfrowej i istotny zasób, który musi być chroniony, poufny i łatwo dostępny. Współczesny globalny rynek zależy od ciągłego przepływu danych między połączonymi sieciami. Inicjatywy związane z transformacją cyfrową i coraz powszechniejsze wykorzystywanie generatywnej sztucznej inteligencji zwiększają narażenie poufnych informacji na ryzyko.

To sprawia, że dane Twojej organizacji są atrakcyjnym i lukratywnym celem dla cyberprzestępców. Niezależnie od branży i wielkości organizacji cyberataki nieustannie narażają firmy i rządy na naruszenie bezpieczeństwa danych, utratę przychodów z powodu przestojów, pogorszenie reputacji i kosztowne kary regulacyjne.

Posiadanie strategii cyberodporności stało się obowiązkiem liderów biznesowych i rządowych, lecz wiele organizacji nie ma pełnego zaufania do swoich rozwiązań w zakresie ochrony danych. Według ankiety Global Data Protection Index 79% osób decyzyjnych w kwestiach IT obawia się, że w ciągu najbliższych 12 miesięcy doświadczy zakłócającego zdarzenia, a 75% obawia się, że istniejące środki ochrony danych w ich organizacjach mogą być niewystarczające, aby poradzić sobie z zagrożeniami ze strony złośliwego oprogramowania i ransomware[1].

Rozwiązanie: Dell PowerProtect Cyber Recovery

Aby zmniejszyć ryzyko biznesowe spowodowane cyberatakami i stworzyć odporniejsze na cyberataki podejście do ochrony danych, można zmodernizować i zautomatyzować strategie w zakresie odzyskiwania i ciągłości działania oraz wykorzystać najnowsze inteligentne narzędzia do wykrywania cyfrowych zagrożeń i obrony przed nimi.



Rozwiązanie Dell PowerProtect Cyber Recovery zapewnia sprawdzoną, nowoczesną, odporną i inteligentną ochronę w celu odizolowania krytycznych danych, identyfikacji podejrzanej aktywności i przyspieszenia odzyskiwania danych, umożliwiając inteligentniejsze odzyskiwanie krytycznych danych w celu szybkiego wznowienia normalnej działalności biznesowej.

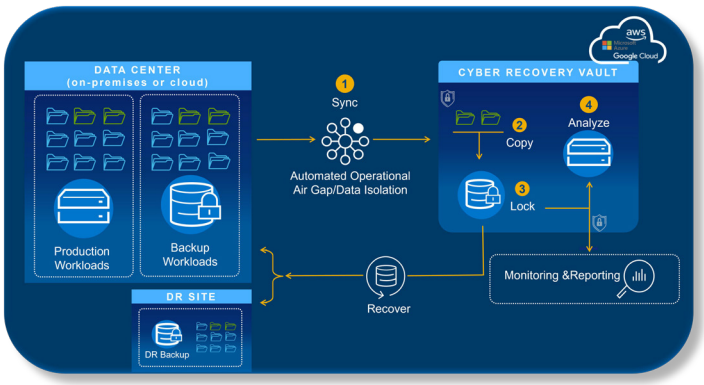
PowerProtect Cyber Recovery — niezmienność, izolacja, inteligencja

Niezmienność danych – PowerProtect Data Domain

PowerProtect Data Domain to podstawowy element rozwiązania Dell PowerProtect Cyber Recovery. Dzięki wielu warstwom zabezpieczeń modelu „zero trust" zapewnia niezmienne kopie zapasowe w celu zapewnienia integralności i poufności danych. Funkcje takie jak sprzętowe źródło zaufania, bezpieczny rozruch, szyfrowanie, blokada retencji, kontrola dostępu oparta na rolach i uwierzytelnianie wieloskładnikowe pomagają zapewnić integralność i możliwość odzyskania danych.

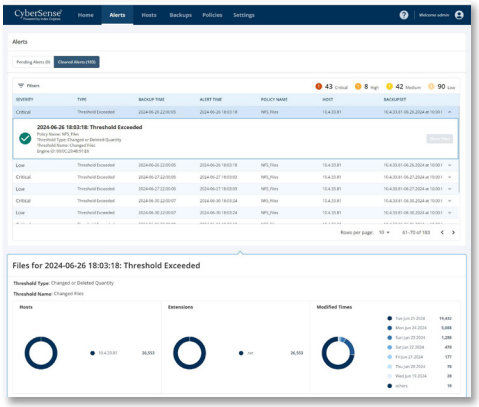
Izolacja – magazyn Cyber Recovery

Magazyn PowerProtect Cyber Recovery stanowi izolowane środowisko odzyskiwania danych, które zapewnia wiele warstw ochrony w celu zagwarantowania odporności na cyberataki i zagrożenia wewnętrzne. Jego operacyjna fizyczna izolacja automatycznie przenosi (synchronizuje) krytyczne kopie zapasowe danych w lokalizację oddaloną od obszarów środowisk produkcyjnych podatnych na ataki, w tym systemów otwartych i komputerów mainframe, czyli do magazynu fizycznie izolowanego. Po zsynchronizowaniu krytycznych danych z magazynem automatycznie tworzona jest niezmienna kopia, co zapobiega modyfikowaniu danych. Obok dedykowanego zarządzania, sieci i usług niezależnych od środowiska produkcyjnego, oddzielne poświadczenia zabezpieczeń i uwierzytelnianie wieloskładnikowe są wymagane do uzyskania dostępu do danych w celu przeprowadzenia operacji odzyskiwania i testowania.



Inteligencja — CyberSense®

PowerProtect Cyber Recovery to pierwsze rozwiązanie, które w pełni integruje rozwiązanie CyberSense® w celu inteligentniejszego odzyskiwania danych po cyberatakach w ramach zabezpieczeń magazynu Cyber Recovery. CyberSense wykracza poza rozwiązania oparte wyłącznie na metadanych. Dzięki analizie całej zawartości rozwiązanie to wykrywa uszkodzenia danych po ataku z dokładnością na poziomie 99,99%[2] oraz umożliwia inteligentne i szybkie przywracanie danych. Rozwiązanie CyberSense wykorzystuje niezmienne kopie zapasowe danych do obserwowania sposobu modyfikowania danych w czasie, a następnie używa uczenia maszynowego opartego na sztucznej inteligencji do wykrywania oznak uszkodzenia wskazujących na atak ransomware. Rozwiązanie CyberSense wykrywa masowe usuwanie, pełne i częściowe szyfrowanie i inne podejrzane zmiany w podstawowej infrastrukturze (w tym Active Directory, DNS itp.), plikach użytkowników i bazach danych wynikające z zaawansowanych ataków. Możliwe jest tworzenie niestandardowych alertów progowych, a w przypadku wykrycia oznak uszkodzenia pulpit nawigacyjny alertów i raporty analityczne po ataku ułatwiają szybką diagnozę skali i skutków ataku, w tym identyfikację czystej kopii danych w celu odzyskania krytycznych systemów.



PowerProtect Cyber Recovery — opcje wdrożenia

Cyber Recovery w środowiskach hybrydowych i wielochmurowych

Krytyczne dane mogą znajdować się w wielu różnych lokalizacjach firmy, lokalnie, w różnych centrach przetwarzania danych lub globalnie w wielu chmurach i regionach. Niezależnie od lokalizacji dane muszą być bezpieczne i nienaruszone na wypadek potrzeby ich odzyskania po cyberatakach.

Rozwiązanie PowerProtect Cyber Recovery jest dostępne i możliwe do wykorzystania za pośrednictwem platform w chmurach publicznych przeznaczonych dla *AWS, Microsoft Azure* i *Google Cloud* w celu zapewnienia szybkiego dostępu do danych w magazynie Cyber Recovery w chmurze. PowerProtect Cyber Recovery automatyzuje synchronizację krytycznych danych między systemami produkcyjnymi a magazynem Cyber Recovery w chmurze publicznej. W przeciwieństwie do standardowych rozwiązań do tworzenia kopii zapasowych opartych na chmurze dostęp do interfejsów zarządzania jest blokowany przez kontrolę sieciową i wymaga oddzielnych poświadczeń zabezpieczeń i uwierzytelniania wieloskładnikowego. Rozproszenie i duplikowanie danych w wielu chmurach może prowadzić do zagrożeń bezpieczeństwa i zgodności, potencjalnych problemów z synchronizacją oraz większych kosztów związanych z zasobami. Takie podejście może również zmniejszyć widoczność w różnych środowiskach, co prowadzi do niewystarczającej ochrony przed stale zmieniającymi się zagrożeniami cybernetycznymi.

Rozwiązanie Dell PowerProtect Cyber Recovery z usługami MultiCloud Data Services oparte na technologii Faction zapewnia jednoczesny dostęp do danych dostawcom rozwiązań chmury publicznej bez szkody dla bezpieczeństwa oraz daje swobodę wyboru dowolnego dostawcy rozwiązań chmurowych i możliwość uniknięcia uzależnienia od jednego dostawcy. Ta bezpieczna usługa zdalnego przechowywania kopii zapasowych to logicznie fizycznie odizolowany magazyn zbudowany na bezpiecznej infrastrukturze obsługującej wiele chmur, który chroni krytyczne dane przed cyberatakami. Gdy wymagane jest odzyskiwanie danych, można przywrócić dane z magazynu do AWS, Microsoft Azure, Google Cloud, Oracle Cloud lub z powrotem do środowiska lokalnego.

Rozwiązanie Dell APEX Protection Storage All-Flash dla Cyber Recovery

Podczas gdy ilość danych krytycznych stale rośnie, możliwość szybkiego i skutecznego odzyskiwania danych po zdarzeniu cybernetycznym ma kluczowe znaczenie dla zapewnienia ciągłości prowadzenia działalności biznesowej i odporności na cyberataki. Organizacje, które poszerzają możliwości zarządzania danymi o znaczeniu krytycznym, muszą wyróżniać się doskonałością w zakresie odzyskiwania danych z izolowanych środowisk odzyskiwania, takich jak magazyn Cyber Recovery. Rozwiązanie Dell APEX Protection Storage All-Flash oparte na zdefiniowanej programowo wersji rozwiązania PowerProtect Data Domain, to uproszczone, energooszczędne i ekonomiczne rozwiązanie do odzyskiwania danych po cyberatakach, które oferuje lepszą analizę CyberSense i możliwości szybkiego przywracania danych w celu spełnienia wymogów organizacji w zakresie umów SLA. Dzięki mniejszej ilości potrzebnego sprzętu, miejsca i energii organizacje mogą przyspieszyć dostęp do danych, zwiększyć wydajność operacyjną i zapewnić integralność danych, co ostatecznie prowadzi do skrócenia przestojów i obniżenia całkowitych kosztów konserwacji.

PowerProtect Cyber Recovery — powrót do działalności biznesowej

Odzyskiwanie i działania zaradcze

PowerProtect Cyber Recovery zapewnia zautomatyzowane procedury przywracania i odzyskiwania w celu szybkiego i niezawodnego wznowienia działania systemów o znaczeniu krytycznym. Odzyskiwanie jest zintegrowane z procesem reagowania na incydenty. Po wystąpieniu zdarzenia zespół reagowania na incydenty analizuje środowisko produkcyjne w celu określenia głównej przyczyny zdarzenia. Rozwiązanie CyberSense dostarcza raporty analityczne po ataku, aby uzyskać dogłębny wgląd w charakterystykę ataku, a także udostępnia listę ostatnich prawidłowych zestawów kopii zapasowych przed uszkodzeniem. Gdy produkcja jest gotowa do wznowienia, rozwiązanie Cyber Recovery zapewnia narzędzia do zarządzania i technologię, która przeprowadza rzeczywiste odzyskiwanie danych.

Planowanie i projektowanie rozwiązań

Usługi Dell Professional Services dla Cyber Recovery pomagają określić, które krytyczne systemy dla działalności biznesowej należy chronić, oraz są w stanie utworzyć mapy zależności powiązanych aplikacji i usług, a także infrastruktury potrzebnej do ich odzyskania. Usługa generuje również wymagania dotyczące odzyskiwania i alternatywy projektowe, a także identyfikuje technologie analizy, hostowania i ochrony danych wraz z uzasadnieniem biznesowym i harmonogramem wdrożenia.

Wnioski

Inicjatywy branżowe, takie jak Sheltered Harbor, wykorzystują rozwiązanie PowerProtect Cyber Recovery do ochrony klientów, instytucji finansowych i zaufania publicznego systemu finansowego Stanów Zjednoczonych na wypadek cyberataku powodującego awarię krytycznych systemów – w tym kopii zapasowych. Rozwiązanie Cyber Recovery z technologią CyberSense, z którego korzystają tysiące klientów, daje liderom biznesowym pewność siebie oraz przyspiesza odzyskiwanie danych w przypadku zagrożenia cybernetycznego. Na podstawie badań Forrester Consulting w przypadku cyberataku rozwiązanie PowerProtect Cyber Recovery pomaga skrócić czas przestoju o 75% oraz czas poświęcany na odzyskiwanie o 80%[3].

Rozwiązanie PowerProtect Cyber Recovery pozwala szybko identyfikować i przywracać znane prawidłowe dane oraz wznowić normalną działalność biznesową po cyberataku. Czas na powrót do działalności biznesowej.

[1] Na podstawie badania „Global Data Protection Index 2024 Snapshot" przeprowadzonego przez firmę Vanson Bourne na zlecenie firmy Dell Technologies. Październik 2023 r.
[2] Na podstawie raportu „Index Engines' CyberSense Validated 99,99% Effective in Detecting Ransomware Corruption" opracowanego przez ESG na zlecenie Index Engines. Czerwiec 2024 r.
[3] Badanie „The Total Economic Impact of Dell PowerProtect Cyber Recovery" przeprowadzone przez Forrester Consulting na zlecenie Dell Technologies w sierpniu 2023 r.

Dowiedz się więcej o rozwiązaniu Dell PowerProtect Cyber Recovery

Skontaktuj się z ekspertem firmy Dell Technologies

Zobacz więcej zasobów

Dołącz do rozmowy pod hasztagiem #PowerProtect