COMMVAULT

OPIS ROZWIĄZANIA

Rozwiązanie Commvault do ochrony i odzyskiwania danych po cyberataku

Wielowarstwowe rozwiązanie do ochrony i odzyskiwania danych oraz wykrywania cyberzagrożeń

Gotowi?

Ataki ransomware, które mają na celu wyłudzenie okupu, nie schodzą z pierwszych stron gazet na całym świecie. Mówią o nich wszyscy, zarówno użytkownicy biznesowi, jak i indywidualni. Zarządy przedsiębiorstw pracują nad planami ochrony przed takimi zagrożeniami oraz usuwania ich skutków. Niestety w przypadku tego typu ataków pytanie nie brzmi „czy", lecz „kiedy" one nastąpią.

Usunięcie skutków ataku ransomware zajmuje firmie średnio 21 dni , czyli aż trzy tygodnie. To jednak za dużo. Zarząd oczekuje, aby plany odtwarzania danych po takim ataku umożliwiały firmie powrót do normalnej działalności w ciągu kilku dni, nie tygodni. Jak by tego było mało, 26% przedsiębiorstw twierdzi, że cyberataki przyniosły szkody ich markom[2].

Wydaje Ci się, że są to trudności nie do pokonania? Mamy dla Ciebie dobrą wiadomość. Commvault od ponad 25 lat pomaga przedsiębiorstwom w ochronie danych i zarządzaniu nimi. To partner, na którego możesz liczyć, jeśli chcesz efektywnie zaplanować ochronę danych i ich odzyskiwanie po ataku ransomware.

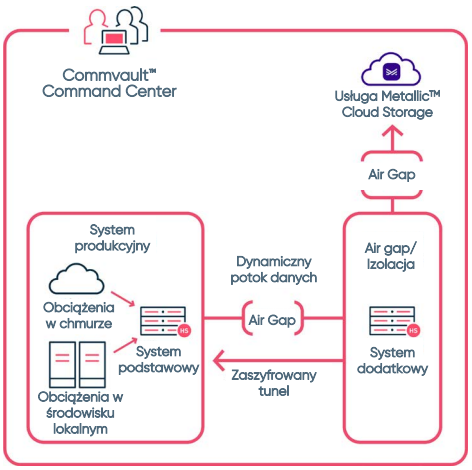
Rozwiązanie Commvault do ochrony i odzyskiwania danych

Commvault oferuje najskuteczniejsze funkcje ochrony i odzyskiwania danych

- Najwięcej typów obsługiwanych aplikacji/systemów
- Najlepsza informacje o danych w ramach infrastruktury
- Najlepsze w branży wsparcie dla platform pamięci masowej.

Rozwiązanie Commvault jest oparte na strategii tworzenia kopii zapasowych 3-2-1 i wzmocnionych zabezpieczeniach hardening. Ośrodek odizolowany za pomocą separacji (ang. air gap) umożliwia szybkie odzyskiwanie danych, a bezpieczne kopie przechowywane w chmurze zapewniają dodatkową ochronę. Oto najważniejsze cechy tego rozwiązania:

1. Wzmocniona infrastruktura w połączeniu ze stosowaniem najlepszych procedur i zaleceń zmniejsza obszar narażony na ataki.
2. *Air gap* izoluje kopie zapasowe od sieci publicznych oraz umożliwia ich segmentację w celu ograniczenia i ochrony dostępu.
3. Uwierzytelnianie i autoryzacja użytkowników oraz kontrolowanie ich działań zapewniają ochronę przed atakami szkodliwego oprogramowania.
4. Integralność danych jest sprawdzana podczas backupów w trakcie ich przesyłania przez sieć i przechowywania.
5. Blokowanie kopii zapasowych, które mogą być modyfikowane tylko przez autoryzowane procesy systemu Commvault, chroni przed atakami ransomware.



Siedem kroków firmy Commvault do zabezpieczenia Twoich danych

1. **Opracowanie planu opartego na strategii wielowarstwowej**
   Plan ten powinien potwierdzać, że dane o znaczeniu krytycznym są odporne na ukierunkowane ataki, a proces ich odzyskiwania jest zautomatyzowany i skoordynowany.
2. **Zapewnienie niezmienności kopii zapasowych w miejscu ich przechowywania**
   Kopie zapasowe powinny być zablokowane, tak aby nie mogły zostać zmodyfikowane ani zaszyfrowane przez szkodliwe oprogramowanie ransomware.
3. **Hardening infrastruktury**
   Należy zmniejszyć obszar narażony na ataki, eliminując wszystkie luki w zabezpieczeniach przy pomocy odpowiednich technologii. Wówczas luki te nie staną się punktami wejścia dla cyberprzestępców.
4. **Hardening aplikacji**
   Obejmuje inteligentną kontrolę dostępu do zasobów, egzekwowanie reguł i monitorowanie używania systemu.
5. **Izolacja danych i air gap**
   Aby zmniejszyć ryzyko ataku, należy odizolować i posegmentować kopie zapasowe oraz umożliwić odtwarzanie danych z danego punktu w czasie przed rozpoczęciem ataku.
6. **Monitorowanie i wykrywanie zagrożeń**
   Łatwe w obsłudze konsole umożliwiają ciągłe monitorowanie stanu bezpieczeństwa systemu, a w przypadku wykrycia podejrzanych i szkodliwych działań - szybkie wysyłanie alertów i podejmowanie odpowiednich środków zaradczych.
7. **Osiągnięcie stanu gotowości do odzyskiwania danych**
   Należy opracować kompleksowy plan ciągłego odzyskiwania danych, obejmujący udokumentowane, zautomatyzowane i przewidywalne etapy tego procesu.

Dowiedz się więcej >

1 Coveware Quarterly Ransomware Report, 1 lutego 2021 r.

2 McAfee The Hidden Costs of Cybercrime 2020

COMMVAULT

OPIS ROZWIĄZANIA

Wielowarstwowe środowisko zabezpieczeń Commvault

Przedsiębiorstwa świadome wagi cyberbezpieczeństwa ufają firmie Commvault. Korzystają z jej rozwiązań, aby w przypadku cyberataku szybko odzyskać dane i przywrócić normalną pracę swoich systemów informatycznych. Commvault stosuje wielowarstwowy model ochrony danych i zarządzania nimi, który każda firma może dostosować do swoich potrzeb. Środowisko zabezpieczeń Commvault jest zgodne ze standardami i najlepszymi procedurami instytutu NIST (National Institute of Standards and Technology).

Wielowarstwowy model zabezpieczeń Commvault obejmuje pięć obszarów: wykrywanie, ochronę, monitorowanie, reagowanie i odzyskiwanie.

Wykrywanie Wszystkie administracyjne funkcje kontrolne są dostępne z jednej konsoli, co pomaga w szybkim wykrywaniu ryzyka i sprawdzaniu zakresu ochrony. Ta **konsola zarządzania** o nazwie Commvault Command Center™ umożliwia rygorystyczną kontrolę dostępu do danych z wykorzystaniem takich metod, jak zatwierdzanie komend przez dwie osoby, weryfikacja danych uwierzytelniających oraz integracja z najlepszymi systemami zarządzania dostępem uprzywilejowanym (PAM).

Ochrona Commvault oferuje znakomite rozwiązania, które pomagają firmom w lepszym zabezpieczeniu danych. Intuicyjne konsole i uproszczone procesy pozwalają **łatwo zmniejszyć obszar narażony na ataki**, zabezpieczyć kopie zapasowe za pomocą separacji (air gap), szybko włączyć chmurę w strategię bezpieczeństwa oraz zapewnić niezmienność kopii zapasowych.

Monitorowanie Łatwe w obsłudze konsole umożliwiają ciągłe monitorowanie stanu bezpieczeństwa środowiska informatycznego. Tylko Commvault udostępnia takie funkcje, **jak wczesne ostrzeganie o podejrzanych lub szkodliwych działaniach** za pośrednictwem jednego interfejsu, aktywne monitorowanie systemu pod kątem nieprawidłowych działań z wykorzystaniem uczenia maszynowego i sztucznej inteligencji, szybkie wykrywanie ataków ransomware za pomocą honeypot oraz śledzenie aktywności i uprawnień użytkowników.

Reagowanie Commvault zapewnia nienaruszone kopie zapasowe, dzięki czemu Klient może u**niknąć przerw w pracy oraz zminimalizować ryzyko** poprzez automatyczne izolowanie podejrzanych plików, zapobieganie wygasaniu kopii zapasowych oraz ochronę własnych aplikacji. Ponadto zasoby i fachowa wiedza udostępniane w ramach usługi Commvault Readiness Solutions umożliwiają Klientowi szybszy powrót do normalnej działalności po utracie danych. Usługa ta obejmuje zaprojektowanie i wdrożenie rozwiązania oraz wsparcie dla środowiska informatycznego.

Odzyskiwanie Commvault zapewnia **najszerszy w branży zakres wsparcia dla aplikacji i systemów**. Dzięki temu Klient może korzystać z tego samego procesu odzyskiwania w odniesieniu do wszystkich danych i obciążeń w ujednolicony sposób, a także odtwarzać dane do środowisk lokalnych i chmurowych oraz wszędzie tam, gdzie są potrzebne. Commvault umożliwia szybkie odtworzenie danych bez ryzyka ponownego zarażenia plików po ataku ransomware,bez ograniczeń związanych z chmurą. Można go zautomatyzować i zapewnić sobie odtwarzanie czystych plików.

Ochrona danych, wykrywanie zagrożeń i usuwanie skutków cyberataków mają ogromne znaczenie dla każdej firmy. Commvault oferuje wielowarstwowe rozwiązanie zabezpieczające, w którym dostępne są najbardziej efektywne na rynku funkcje ochrony i odtwarzania danych. W przypadku cyberataku umożliwia ono Klientowi szybkie odzyskanie danych i wznowienie działalności biznesowej, a przede wszystkim zapewnia mu prawdziwe poczucie bezpieczeństwa.

Dowiedz się więcej o możliwościach wykorzystania rozwiązań Commvault do ochrony przed zagrożeniami cybernetycznymi. Zapraszamy na stronę commvault.com/ransomware >

COMMVAULT Be ready™

commvault.com | 888.746.3849