OCHRONA I ODZYSKIWANIE DANYCH OD A DO Z

Brief rozwiązania

PRZEGLĄD

Zagrożenia cybernetyczne stają się z każdym dniem coraz bardziej złożone. To, co kiedyś było praktyką samotników, przekształciło się w nową formę cyfrowej przestępczości zorganizowanej, która z kolei rodzi bardziej wyrafinowane technologie i taktyki, ponieważ cyberprzestępcy próbują infiltrować sieci i łańcuchy dostaw. Kiedy zagrożenia cybernetyczne ewoluują, magazyny danych pęcznieją, a zasoby działów IT kurczą się, współczesne organizacje potrzebują coraz lepszych sposobów na zabezpieczanie swoich danych w ciągle zmieniającym się środowisku. Chociaż tradycyjne rozwiązania do ochrony danych mogą odgrywać znaczną rolę w odzyskiwaniu sprawności po ataku, są to narzędzia reaktywne o wąskim zakresie działania – a to nie wystarczy do zapewnienia znacznej redukcji ryzyka.

Tylko Commvault dostarcza niezawodnych środków kontroli i narzędzi z zakresu bezpieczeństwa, które współpracują ze sobą, aby proaktywnie odkrywać zagrożenia, minimalizować ryzyko, zarządzać danymi i dostępem do nich, a także wspierać inteligentne, oparte na bogatszych informacjach rezultaty procesu odzyskiwania. Narzędzie do ochrony przed atakami ransomware i odzyskiwania po ataku Commvault® gwarantuje, że Twoje dane będą **zabezpieczone**, **chronione** i **odzyskiwalne** – w dowolnym miejscu. Nasze podejście do ochrony danych od A do Z zapewnia odpowiedni zakres możliwości wykrywania zagrożeń oraz zabezpieczania i odzyskiwania danych, aby gwarantować proaktywną, warstwową ochronę w środowiskach chmurowych, lokalnych i SaaS. Zapewniamy bezpieczeństwo w oparciu o nasze trzy filary ochrony danych:

- **Dane, zabezpieczone:** Wzmocniona, niezmienna architektura o zerowym zaufaniu z wbudowanymi protokołami bezpieczeństwa w celu zabezpieczenia danych, zapobiegania niepożądanemu dostępowi do danych i zapewnienia zgodności w obliczu ewoluujących zagrożeń cybernetycznych.
- **Dane, chronione:** Wczesne ostrzeganie i szczegółowe monitorowanie nowej generacji w celu wykrywania i neutralizowania zagrożeń typu zero-day i zagrożeń wewnętrznych, zanim wyrządzą one szkody – tym samym ogranicza się naruszenia, zawężając okna narażenia na atak i szybciej sygnalizując złośliwą aktywność, aby zmniejszyć potrzebę odzyskiwania danych.
- **Dane, odzyskiwalne:** Proaktywne i niezawodne możliwości odzyskiwania danych w najszerszym w branży pokryciu obciążeń. Potwierdzone skrócenie przestojów, zapobieganie utracie danych i przyspieszanie czasu reakcji, co przekłada się na niezrównaną ciągłość biznesową.

ZAKRES OD A DO Z

A „Air Gap” – szczelina lub „ściana” powietrzna chroniąca niezmienne kopie zapasowe danych.

Z „Zero Trust” – zasady zerowego zaufania oraz nieustanne monitorowanie obejmujące całe środowiska kopii zapasowych i środowiska produkcyjne.

Ochrona danych od dawna jest nazywana ostatnią linią obrony firmy, która wchodzi do gry, gdy doszło już do szkód i strat. Commvault zmienia ten paradygmat, dostarczając unikatowe, proaktywne i innowacyjne zdolności w zakresie ochrony i bezpieczeństwa, które zapobiegają szkodom, minimalizują ryzyko i eliminują czas przestoju – jednolicie, w całym magazynie danych (lokalnie, w chmurze i w środowiskach SaaS). Możesz szybko i prosto chronić środowiska danych od A do Z, korzystając z tych funkcji:

Szczelina powietrzna: Ochroń kopie zapasowe danych, tworząc warstwę zabezpieczenia chmury, ograniczając dostęp do kont i zapewniając izolację danych. Wszystkie rozwiązania są w pełni zintegrowane z naszym pakietem ochrony danych (w tym funkcją tworzenia i odzyskiwania kopii zapasowych, przechowywania danych w chmurze oraz skalowania zintegrowanych urządzeń).

AI i automatyzacja pomagają w zarządzaniu kopiami danych poprzez wykorzystanie uczenia maszynowego i analiz opartych na danych historycznych, dzięki czemu można podejmować decyzje w oparciu o lepsze informacje.

Analiza danych: Proste identyfikowanie wrażliwych zestawów danych w celu zapobiegania nadmiernemu narażeniu i usuwania złośliwego oprogramowania, co zapobiega ponownej infekcji i utrzymuje dane „w czystości".

Wczesne ostrzeganie: Zaawansowane funkcje wykrywania zagrożeń cybernetycznych umożliwiają detekcję wewnętrznych i zewnętrznych ataków w środowisku produkcyjnym – zanim ataki dosięgną danych.

Globalna widoczność: Szczegółowe dane umożliwiające podejmowanie działań w zakresie danych z wykorzystaniem ujednoliconej platformy. Zastosuj standaryzację zabezpieczeń, uprość zarządzanie ryzykiem względem danych i zyskaj kontrolę nad globalnymi operacjami tworzenia kopii zapasowych, korzystając z tego innowacyjnego rozwiązania SaaS.

Niezmienność danych: Skorzystaj z wzmocnionych i zaawansowanych środków kontroli, aby zagwarantować, że dane nigdy nie zostaną zmanipulowane, usunięte, zmodyfikowane lub zmienione.

Ekosystem bezpieczeństwa: Integracje dostarczające zróżnicowanych opcji ochrony i zabezpieczania danych dla zintegrowanych środowisk IT, np. Microsoft Sentinel i CyberArk.

Architektura zerowego zaufania: Skorzystaj z wieloskładnikowego i wieloosobowego uwierzytelniania; zarządzania dostępem uprzywilejowanym (PAM); oraz zarządzaniem tożsamościami i dostępem (IAM) w narzędziach, takich jak CyberArk, YubiKey i narzędzia biometryczne (np. AAL3).

OCHRONA PRZED ATAKAMI RANSOMWARE I ODZYSKIWANIE PO ATAKU COMMVAULT

Dzisiejsze wszechobecne zagrożenia cybernetyczne oznaczają potrzebę zmiany podejścia do ochrony danych w celu wyprzedzenia atakujących. Wyposaż firmę w proaktywne zdolności zabezpieczania danych, przewidywania zagrożeń oraz dostarczania niezawodnego odzyskiwania danych – w obliczu dowolnego zagrożenia. Sprawdź produkty i rozwiązania Commvault, aby rozszerzyć możliwości ochrony od A do Z i odzyskiwania danych w przypadku ataków ransomware:

Complete Data Protection oraz Metallic® SaaS Backup to zaawansowane opcje obsługi kopii zapasowych danych, które chronią dane i umożliwiają ich odzyskiwanie, spełniając wymagania zawarte w umowach o poziomie świadczonych usług (SLA).

Commvault® Risk Analysis lokalizuje wrażliwe dane i zarządza nimi, aby chronić dane umożliwiające identyfikację poszczególnych osób przed zagrożeniami wewnętrznymi i zewnętrznymi, gwarantując zgodność z umowami SLA.

Commvault® Threat Scan umożliwia identyfikowanie i reagowanie na incydenty w krótszym czasie, unikanie ponownej infekcji plików oraz szybsze przywracanie danych objętych atakiem.

Metallic® ThreatWise™ korzysta z opatentowanego rozwiązania wczesnego ostrzegania, które umożliwia ujawnianie luk zero-day i nieznanych zagrożeń cybernetycznych, zanim spowodują szkody. Reaguj szybciej – przed zaszyfrowaniem, wyciekiem lub eksfiltracją danych.

Od szczeliny powietrznej po zasady zerowego zaufania – Commvault chroni Cię od A do Z, korzystając z kluczowych zdolności: **Dane, zabezpieczone**; **Dane, chronione**; oraz **Dane, odzyskiwalne**. Z rozwiązaniami Commvault zyskujesz ochronę przed atakami ransomware i gotowość do odzyskiwania danych po ataku.

Dowiedz się więcej o ochronie od A do Z oferowanej przez Commvault

enua COMMVAULT

Z Commvault masz wszystko, co potrzebne do ochrony

Zapraszam do kontaktu

Anna Siennicka
Key Account Manager

anna.siennicka@enue.pl
Tel: 789 306 126

enue COMMVAULT®

Wspieramy naszych klientów na każdym etapie projektu