COMMVAULT

ARTYKUŁ PRZEGLĄDOWY

Jak skutecznie chronić dane i firmę w czasie nasilenia zagrożeń cybernetycznych

Sprawdzona technologia, ciągłe monitorowanie zagrożeń, regularne aktualizacje oraz edukacja użytkowników to cechy oprogramowania do ochrony i zarządzania danymi, jakiego potrzebuje Twoja firma.

Zagrożenia cybernetyczne, w tym ataki typu ransomware, przybrały na sile do tego stopnia, że nie zadajemy sobie już pytania, „czy", lecz „kiedy" nastąpią. Jeśli firma w przypadku takiego ataku chce odzyskać swoje dane bez konieczności płacenia okupu, musi znaleźć dostawcę rozwiązań zabezpieczających, któremu może zaufać. Właściwe rozwiązanie wymaga zaangażowania odpowiednich technologii, ludzi i procesów.

Commvault pracuje w stanie ciągłej gotowości, podobnie jak dyrektorzy ds. bezpieczeństwa informatycznego w przedsiębiorstwach. Szybko reagujemy na potrzeby Klientów, oferując im odpowiednie produkty i usługi. Commvault zyskał znakomitą reputację jako zaangażowany, zaufany partner. Wielu Klientów potwierdza naszą innowacyjność oraz zdolność do szybkiego podejmowania działań pod presją, w świecie stale zagrożonym atakami ransomware.

Zapewnienie bezpieczeństwa danych jest dla firmy Commvault celem strategicznym, realizowanym za pomocą takich rozwiązań, jak zabezpieczenia wielowarstwowe, zaawansowane metody wykrywania zagrożeń czy mechanizmy szybkiego odzyskiwania danych w przypadku naruszenia ich bezpieczeństwa, np. naruszenia poufności lub ataku ransomware.

Przedsiębiorstwa potrzebują narzędzi, które pomogą im w ciągłej ocenie stanu gotowości do odzyskiwania danych. Narzędzia takie powinny pozwalać na wykrywanie i rozwiązywanie problemów, automatyczne testowanie możliwości odzyskiwania danych i aplikacji biznesowych, a także ciągłe umacnianie bezpieczeństwa środowiska informatycznego i obniżanie poziomu ryzyka.

Jak chronić same kopie zapasowe przed zagrożeniami? Najczęściej stosuje się w tym celu odpowiedni poziom izolacji, oparty np. na separacji danych (ang. air-gap), oraz zabezpieczeniu przed zmianami kopii zapasowych. Commvault ma podobne podejście. Z powodzeniem wykorzystujemy zabezpieczenia oparte na trwałych backupach, segregacji geograficznej i air-gap zarówno w przypadku lokalnych, jak i chmurowych lokalizacji przechowywania kopii zapasowych. Co więcej umożliwiamy Klientom używanie albo naszych urządzeń typu appliance lub własnych pamięci masowych.

Zapewnienie bezpieczeństwa danych w sposób, który nie utrudnia sprawnego administrowania oprogramowaniem, nie zawsze jest łatwe. Commvault pomaga w rozwiązaniu tego problemu. Chroni dane przed kradzieżą, naruszeniem prywatności, uszkodzeniem lub usunięciem przez sprawców wewnętrznych i zewnętrznych, działających umyślnie lub bez złych zamiarów.

Model zabezpieczeń AAA (ang. authentication, authorization, accounting uwierzytelnianie, autoryzacja i audytowanie) umożliwia ocenę każdego oprogramowania pod względem bezpieczeństwa. Jest on znany i ceniony w społeczności specjalistów ds. bezpieczeństwa. Commvault korzysta z niego w celu oceny, doskonalenia i prezentowania swoich rozwiązań oraz wykazywania ich zgodności z przepisami branżowymi i najlepszymi praktykami. Zgodnie z zasadą zerowego zaufania zdefiniowaną w normie NIST SP 800-207 Commvault udostępnia swoim Klientom szereg usług umożliwiających segmentacje i/lub izolowanie danych, kontrolę tożsamości użytkowników, zapewnianie dostępu w oparciu o najmniejsze wymagane uprawnienia, ochronę przed skutkami błędów użytkowników, a także pełne i szczegółowe rejestrowanie zdarzeń w dzienniku oraz przeprowadzanie audytu. Te mechanizmy zabezpieczające działają w przypadku wszystkich metod dostępu do systemu interfejsu użytkownika, wiersza komend lub interfejsu API.

Zagrożenia nie zawsze pochodzą z zewnątrz, nie w każdym przypadku sąwynikiem kradzieży danych uwierzytelniających lub innych celowych działań hackerów. W celu walki z zagrożeniami wewnętrznymi Commvault wprowadził specjalny mechanizm kontrolny: zadania administracyjne, które mogą stanowić ryzyko dla bezpieczeństwa danych, są zatwierdzane przez co najmniej dwóch administratorów z wybranej grupy uprawnień (zgodnie z zasadą „czworga oczu").

Rozwiązanie do odtwarzania danych jest skuteczne tylko wtedy, jeśli sprawdza się w różnych scenariuszach. Czasem wystarczy przywrócenie wcześniejszych instancji systemu sprzed uszkodzenia danych, innym razem nie obejdzie się bez pełnego odtworzenia aplikacji biznesowych w nowej lokalizacji. W osiągnięciu stanu gotowości pomaga zaprojektowanie procesów odtwarzania danych w różnych środowiskach oraz udostępnienie prostych zautomatyzowanych funkcji, które umożliwiają testowanie i sprawdzanie poprawności tych procesów w różnych przypadkach. Automatyczne przetestowanie procesu odzyskiwania newralgicznych danych i aplikacji zapewnia nie tylko lepszy poziom ochrony i zgodności z obowiązującymi przepisami, lecz także poczucie bezpieczeństwa.

Commvault opracował metody, które umożliwiają uzupełnienie typowego oprogramowania IT security o funkcje monitorowania i wykrywania zagrożeń, uwzględniające najważniejsze aspekty architektury platformy backupu . Algorytmy uczenia maszynowego wykrywają nieprawidłowości w działaniach dotyczących plików, natomiast pliki instalowane jako wabiki (ang. honeypot) na cyberprzestępców szybko ostrzegają o możliwości ataków ransomware. Wraz z tymi narzędziami użytkownik zyskuje funkcje wczesnego ostrzegania bez ponoszenia dodatkowych kosztów lub nakładów pracy związanych z zarządzaniem.

W poniższej tabeli podsumowano najważniejsze zagrożenia oraz oferowane przez Commvault sposoby przeciwdziałania im.

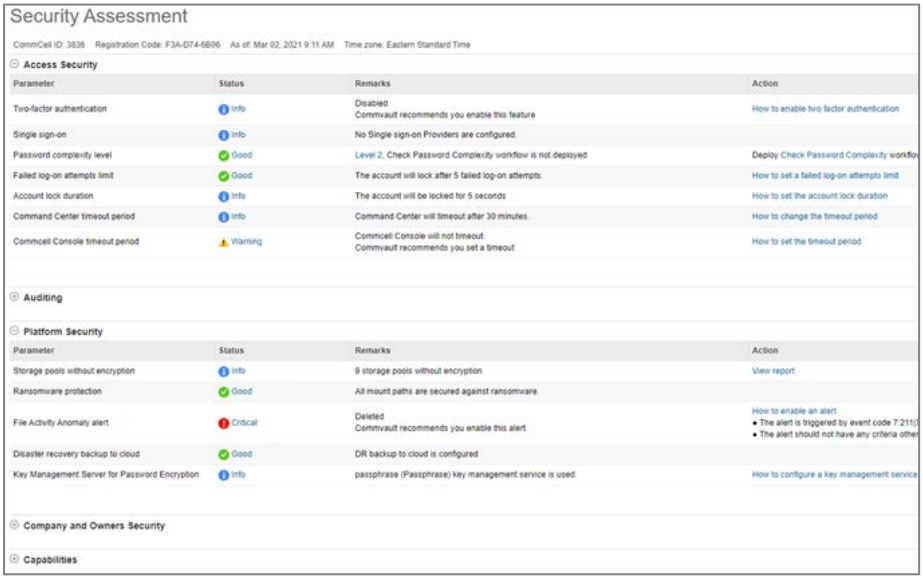
Zagrożenie	Strategia
Atak ransomware w celu zniszczenia kopii zapasowych	Zabezpieczenie kopii zapasowych oraz zapewnienie ich niezmienności dla każdego konta administratora. Modyfikacje możliwe tylko w przypadku zweryfikowanych procesów systemu Commvault. Dodatkowa ochrona zapewniona przez cyfrowe podpisywanie plików binarnych systemu Commvault oraz wymóg uwierzytelniania przy użyciu certyfikatu w przypadku przełączania się między komponentami systemu Commvault.
Atak cyberprzestępców w celu przejęcia haseł, polityk i danych	Bezpieczne uwierzytelnianie za pomocą zabezpieczeń wieloskładnikowych oraz precyzyjnej, opartej na rolach blokadzie dostępu do odpowiednich systemów. Szyfrowanie danych z zarządzaniem kluczami zewnętrznymi. Przepływ pracy kontrolowany zgodnie z zasadą czworga oczu, chroniący przed szkodliwymi działaniami użytkowników z uprawnieniami administratora.
Dostęp do kopii zapasowych przez osobę podszywającą się pod administratora	Oprócz zasady czworga oczu i szczegółowej blokady dostępu opartej na rolach - rejestracja każdego dostępu i każdej wprowadzonej zmiany, a w przypadku zmian o znaczeniu krytycznym – wysyłanie alertów do wybranego systemu. Opcja blokady prywatności chroniąca dane wrażliwe i poufne poprzez uniemożliwienie administratorowi ich przeglądania i odtwarzania.
Przypadkowe usunięcie danych przez administratora	Stosowanie wszystkich zabezpieczeń, które chronią przed cyberprzestępcami i osobami podszywającymi się pod administratorów, również w celu eliminowania potencjalnych błędów administratora.
Zgodność z regulacjami dotyczącymi bezpieczeństwa danych i zarządzania logami	Wprowadzenie przez firmę reguł, które pomogą jej w zachowaniu zgodności z obowiązującymi przepisami prawa i regulacjami, co zwykle dotyczy przechowywania logów przez dłuższy czas. Możliwość przechowywania plików logów z serwerów, punktów końcowych i urządzeń sieciowych w sposób niezależny od ogólnych reguł przechowywania kopii zapasowych.

Niniejszy przewodnik obejmuje najważniejsze sprawdzone procedury dotyczące bezpieczeństwa, używane przez naszych Klientów na całym świecie. Procedury te są wdrażane w ramach procesu ciągłych udoskonaleń i innowacji, którego celem jest zapewnienie ochrony danych i gotowości do ich odzyskiwania. Ilość przetwarzanych danych stale rośnie, a środowiska, w których są one przetwarzane, stają się coraz szersze, od otwartych systemów pamięci masowej po chmurę.

Zalecenia dotyczące bezpieczeństwa danych

Zabezpieczenia danych pomagają przedsiębiorstwom w ochronie przed zagrożeniami cybernetycznymi, w tym kradzieżą danych i atakami ransomware, oraz w kontroli dostępu do najważniejszych informacji. Oferowane przez Commvault inteligentne usługi przetwarzania danych obejmują zaawansowane mechanizmy wykrywania zagrożeń i nieprawidłowości. Stanowią one element ochrony wielowarstwowej, dzięki której dane są dużo bezpieczniejsze. Podczas gdy media informują na pierwszych stronach o kolejnych atakach ransomware, Commvault pomaga firmom w zmniejszeniu ryzyka takich incydentów, a jeśli do nich dojdzie - w szybszym odzyskaniu danych.

Konsola oceny stanu bezpieczeństwa



Na początku należy prawidłowo zidentyfikować i ocenić czynniki ryzyka oraz luki w zabezpieczeniach. Konsola oceny stanu bezpieczeństwa (Security Health Assessment Dashboard), dostępna zarówno w rozwiązaniu Commvault Cloud Metrics Reporting, jak i Commvault Command CenterTM, szybko dostarcza zalecenia i rekomendacje pomagające w opracowaniu planu działania. Na konsoli tej dostępne są wszystkie zalecane mechanizmy kontrolne i ustawienia, które można szybko wdrożyć, korzystając z funkcji interaktywnych. Więcej informacji na ten temat można znaleźć w artykule „Usprawnienie zarządzania ryzykiem za pomocą konsoli oceny stanu bezpieczeństwa" (Improving risk management with the Commvault Security Health Assessment Dashboard).

Opracowanie planu opartego na strategii wielowarstwowej

Commvault stosuke powszechnie znaną zasadę, że wielowarstwowa strategia jest podstawą skutecznej ochrony danych, a gotowość do ich odzyskiwania ma znaczenie krytyczne. Newralgiczne dane firmy powinny być odporne na ukierunkowane ataki, które mają na celu zniszczenie zarówno ich kopii podstawowych, jak i zapasowych, natomiast proces odzyskiwania danych zautomatyzowany i w miarę możliwości skoordynowany. Zakres każdego tworzonego przez firmę planu musi być na tyle szeroki i głęboki, aby dotarł do wartościowych danych niezależnie od tego, gdzie się znajdują. Powinien obejmować nie tylko centralne serwery i aplikacje działające w całej firmie, lecz również laptopy, pliki w różnych formatach na różnych nośnikach oraz specyficzne aplikacje.

Zapewnienie niezmienności kopii zapasowych w miejscu ich przechowywania

Bardzo ważne jest zapewnienie niezmienności kopii zapasowych, tak aby nie mogły one być modyfikowane ani szyfrowane przez szkodliwe oprogramowanie ransomware. Taka funkcjonalność powinna być dostępna bez znaczących kosztów dla wszystkich danych znajdujących się w środowisku informatycznym firmy, z możliwością aktywowania dla wybranej pamięci masowej (dotyczy to zarówno środowisk lokalnych i chmurowych, jak i rozwiązań Commvault HyperScale™). Takie rozwiązanie jest niewątpliwie bardziej korzystne niż oparte tylko na modelu air-gap, a przy tym nie wiąże się z dodatkowymi kosztami i komplikacjami.

Funkcja niezmienności kopii zapasowych jest oparta na sprawdzonych metodach, które ograniczają operacje zapisu i usuwania, a tym samym zabezpieczają pliki na chronionych ścieżkach przed modyfikacją przez hakerów lub szkodliwe oprogramowanie. Commvault niedawno przetestował niezawodność i efektywność tej funkcji za pomocą techniki RIPlace bypass, która może złamać wiele zabezpieczeń punktów końcowych. Rozwiązanie Commvault okazało się jednak odporne na tę technikę.

Oprócz zalecanej strategii wielowarstwowej niektórzy klienci decydują się również na wdrożenie dodatkowych strategii w celu osiągnięcia jeszcze lepszej ochrony. Przykładem - w przypadku niektórych danych - jest tworzenie kopii do jednokrotnego zapisu i wielokrotnego odczytu (ang. write once, read many - WORM) w środowisku lokalnym lub chmurze, a także wdrażanie strategii izolacji opartych na air-gap. W rozwiązaniu Commvault funkcje takie można łatwo wdrożyć w oparciu o reguły, co obejmuje segmentację sieci, szyfrowane topologie sieci, bramy i zapory ogniowe (firewall). Rozwiązanie to umożliwia również automatyzację, która umożliwia rozłączenie sieci i serwera.

Hardening infrastruktury

Wzmocnienie (ang. hardening) infrastruktury zgodnie z odpowiednimi zasadami jest ważne w każdym środowisku, w którym działa oprogramowanie. Główne komponenty rozwiązania Commvault są powiązane z systemem operacyjnym, bazą danych, aplikacją i technologią serwera WWW. Wszystkie słabe punkty zabezpieczeń w tych obszarach muszą więc zostać usunięte, aby nie stały się punktami wejścia dla cyberprzestępców.

- **Stosowanie zaleceń dotyczących wzmocnienia bezpieczeństwa** – rekomendacje dotyczące wzmocnienia bezpieczeństwa oparte na standardach instytutu NIST (National Institute of Standards and Technology) są wdrażane automatycznie.
- **Podpisywanie plików binariów z uwzględnieniem zewnętrznych bibliotek** – środowisko zabezpieczeń Commvault umożliwia cyfrowe podpisywanie plików binarnych, tak aby nie zostały one zmodyfikowane przez cyberprzestępców. Wszelkie biblioteki stron trzecich są regularnie aktualizowane z uwzględnieniem zgłaszanych luk
- **Wzmocnienie bezpieczeństwa zgodne ze standardem CIS Level 1** – oprogramowanie Commvault przeszło pomyślnie test zgodności z normą Center for Internet Security (CIS) Level 1.

Wzmacnianie zabezpieczeń aplikacji poprzez uwierzytelnianie, autoryzację i audytowanie

Model zabezpieczeń AAA (ang. authentication, authorization, accounting - uwierzytelnianie, autoryzacja i audytowanie) umożliwia inteligentne kontrolowanie dostępu do zasobów komputerowych, egzekwowanie reguł i monitorowanie używania systemu. Kombinacja tych procesów jest uważana za niezbędny element efektywnej ochrony sieci i zarządzania nią. Commvault udostępnia bezpieczny, niezawodny i kompleksowy zestaw funkcji w każdym z tych trzech obszarów.

COMMVAULT

ARTYKUŁ PRZEGLĄDOWY

Kontrola dostępu za pomocą środowiska zabezpieczeń AAA

Uwierzytelnianie	Autoryzacja	Audytowanie
Sprawdzanie uprawnień i udzielanie dostępu	Sprawdzanie wymaganego poziomu dostępu	Śledzenie i audyt dostępu i innych działań

Uwierzytelnianie

Proces uwierzytelniania jest oparty na unikalnym zbiorze kryteriów, na podstawie których każdy użytkownik może uzyskać dostęp do systemu. Commvault udostępnia metody uwierzytelniania wieloskładnikowego, które znacznie zmniejszają prawdopodobieństwo podszycia się osoby nieuprawnionej pod użytkownika.

- **Bezpieczny protokół LDAP (Lightweight Directory Access Protocol)** – protokół ten obsługuje katalog Active Directory oraz generyczne serwery tożsamości LDAP.
- **Zewnętrzni dostawcy tożsamości** – są oni obsługiwani za pomocą bezpiecznych protokołów, takich jak Open Authorization (OAuth) i Security Assertion Markup Language (SAML).
- **Uwierzytelnianie wieloelementowe** – jest ono oparte na danych logowania i wykorzystuje aplikację uwierzytelniającą, smart karty oraz sprzętowe klucze uwierzytelniania.
- **Uwierzytelnianie oparte na certyfikacie** – dzięki tej funkcji infrastruktura Commvault chroni konto przed osobami podszywającymi się pod użytkownika (ang. spoofing).
- **Obsługa wielu użytkowników** – stosowana jest mikrosegmentacja administracyjna i sekcjonowanie dostępu.
- **Zarządzanie dostępem uprzywilejowanym (Privilege Access Management – PAM) za pomocą technologii CyberArk** – funkcja ta umożliwia centralne przechowywanie, organizowanie i zabezpieczanie danych uwierzytelniających, w tym danych uwierzytelniających konta usługi oraz sesji logowania administratora, a także zarządzanie nimi bez narażania haseł na ryzyko.

Autoryzacja

Następnym krokiem po uwierzytelnieniu użytkownika jest udzielenie mu autoryzacji do wykonania określonych zadań. W tym zakresie Commvault udostępnia bogaty zakres funkcji:

- **Zabezpieczenie dostosowane do roli** – można zarządzać uprawnieniami na podstawie ról przypisanych do użytkowników i ich grup (również w przypadku środowisk obsługujących wielu użytkowników), a także ograniczyć funkcjonalność i zakres serwerów aplikacji i zbiorów danych, do których użytkownik może uzyskać dostęp i którymi może zarządzać.
- **Przepływy pracy z podwójną autoryzacją** – w przypadku zadań administracyjnych, takich jak usuwanie zbiorów danych, Klientów, danych odzyskanych, lokalizacji docelowych, stanowisk i reguł stosowana jest zasada czworga oczu.
- **Hasło dostępu i blokada prywatności** – obowiązuje zasada, zgodnie z którą administratorzy zarządzają danymi, ale nie powinni przeglądać ani odtwarzać danych, za które nie są odpowiedzialni. Odtwarzać dane może tylko właściciel zbioru danych na poziomie osoby, działu lub firmy, używając wymaganego hasła.
- **Szyfrowanie danych** – stosowane jest szyfrowanie zgodne z certyfikatem FIPS (Federal Information Processing Standards) oraz ponad 6 technologii szyfrowania, w tym AES 256. Dane są szyfrowane od pierwszego dotknięcia, przez cały cykl zarządzania nimi.
- **Zarządzanie kluczami szyfrowania** – stosowany jest wbudowany system zarządzania kluczami (KMS) lub zewnętrzny system KMS strony trzeciej (np. kompatybilny system Key Management Interoperability Protocol (KMIP), AWS KMS lub Azure Key Vault) oraz hasło.
- **Szyfrowanie sieci** – obsługiwane jest enkapsulacja protokołu HTTPS, technologia TLS 1.2 oraz serwer proxy/brama.
- **Odwzorowywanie portów stron trzecich (TPPM)** – stosowane jest tunelowanie komunikacji z zewnętrznymi aplikacjami za pośrednictwem portów sieci Commvault, co znacznie upraszcza wdrażanie systemów w bezpiecznym środowisku.
- **Obsługa kopii WORM** – Reguły WORM (ang. write once, read many kopie do jednokrotnego zapisu i wielokrotnego odczytu) stosowane do kopii danych umożliwiają korzystanie z praw do usuwania danych oraz wprowadzenie ustalonych okresów przechowywania danych.
- **Wsparcie dla usług WORM w chmurze** –pamięć masowa różnych rodzajów (bucket, obiektowa) jest obsługiwana w zakresie konfiguracji WORM.

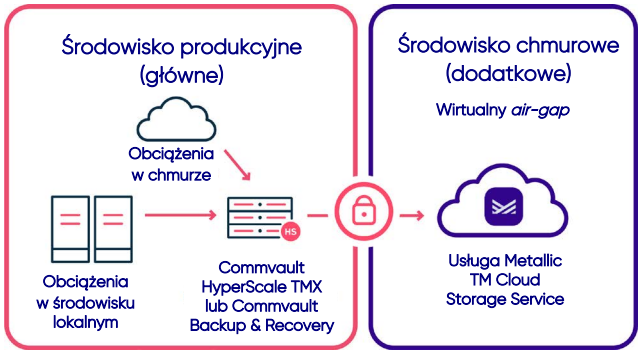
Audytowanie

W ramach audytowania należy rejestrować każdy przypadek uzyskania dostępu do systemu przez użytkownika oraz wszystkie jego działania z uwzględnieniem wymagań dotyczących bezpieczeństwa. Niezbędne jest również tworzenie raportów umożliwiających śledzenie takich działań oraz generowanie alertów w przypadku wystąpienia określonych zdarzeń. W związku z tym należy odpowiedzieć na następujące pytania:

- **Kto zbyt często uzyskuje dostęp do systemu?** Liczba przypadków uzyskania dostępu do systemu za pośrednictwem interfejsu użytkownika, wiersza poleceń i interfejsu API jest śledzona i raportowana.
- **Jak został wykorzystany dostęp do systemu?** Tworzony jest kompletny zapis kontrolny dotyczący uzyskania przez użytkownika dostępu do systemu oraz podejmowanych przez niego działań.
- **W jakich przypadkach uprawnienia dostępu mogą zostać wycofane?** System będzie zgłaszać do usunięcia użytkowników, którzy nie korzystali ze swojego prawa dostępu przez określony czas.
- **Które dane nie są szyfrowane?** Zalecenia w tym zakresie są zwykle oparte na raporcie, który potwierdza status szyfrowania.

Izolacja danych i *air-gap*

Separacja (ang. *air gap*) to koncepcja związana z architekturą ochrony danych, która zmniejsza ryzyko ataków i umożliwia odtwarzanie danych do określonego punktu w czasie przed rozpoczęciem ataku. Commvault skutecznie zmniejsza ryzyko replikacji zarażonych danych w architekturze kopii zapasowych. Wykorzystuje przy tym takie środki, jak trwałe kopie zapasowe, reguły bezpieczeństwa WORM stosowane okresowo do kopii danych oraz wyłączanie funkcji usuwania danych na cały okres ich obowiązkowego przechowywania. Ponadto Commvault wprowadził inne usprawnienia i ulepszenia, takie jak fizyczna kontrola dostępu w każdym rozwiązaniu, rozszerzone środki zabezpieczające, uproszczenie procesów i obniżenie kosztów.



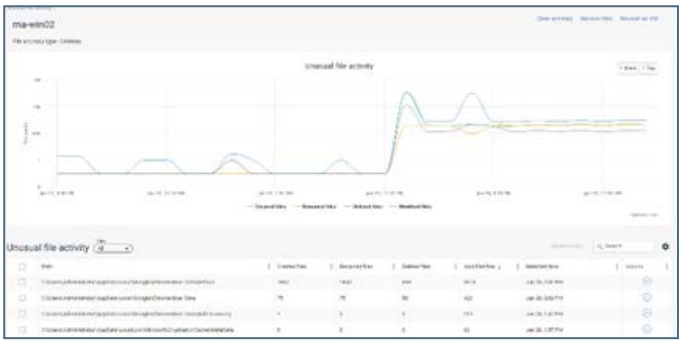
- **Koordynacja oparta na *air-gap*** – automatyzacja przepływów pracy umożliwia rozłączenie sieci i serwera.
- **Segmentacja sieci** – mechanizmy zabezpieczeń sieci blokują zarówno fizycznie, jak i logicznie dostęp z zewnątrz do dodatkowych lokalizacji przechowywania kopii zapasowych.
- **Szyfrowanie topologii sieci** – reguły sieci Commvault umożliwiają odizolowanie komunikacji oraz utworzenie zaszyfrowanych tuneli wychodzących z odizolowanej docelowej lokalizacji przechowywania kopii zapasowych. Bramy Commvault mogą automatycznie kontrolować stałe połączenia.
- **Łatwe wdrażanie bezpiecznej i skalowalnej pamięci masowej w chmurze** – usługa MetallicTM Cloud Storage Service (MCSS) to „przycisk łatwego uruchamiania", który zapewnia dostęp do bezpiecznej (odseparowanej przez air-gap) pamięci masowej w chmurze na potrzeby dodatkowych kopii - przy przewidywalnym koszcie. Nie jest przy tym wymagana dodatkowa infrastruktura.

Lepsza ochrona przed atakami ransomware oparta na technologiach izolacji danych i air-gap. Czytaj >

Monitorowanie i wykrywanie zagrożeń

Wielu specjalistów zaleca stosowanie warstwowej strategii obrony przed szkodliwym oprogramowaniem i atakami ransomware. Commvault wbudował takie możliwości w swoje oprogramowanie zabezpieczające i polityki zabezpieczeń, co zapewnia użytkownikom znaczne korzyści bez zwiększania ogólnych kosztów zarządzania.

- **Monitorowanie aktywności systemu plików** – wykorzystanie danych historycznych i algorytmów uczenia maszynowego umożliwia wykrywanie odmiennych statystycznie zachowań systemu plików.
- **Monitorowanie plików będących wabikami (ang. *honeypot*) na oszustów** – ukryte pliki, które są atrakcyjne dla sprawców ataków ransomware, więc mogą łatwo paść ich ofiarą, są monitorowane pod kątem zmian w sygnaturach.

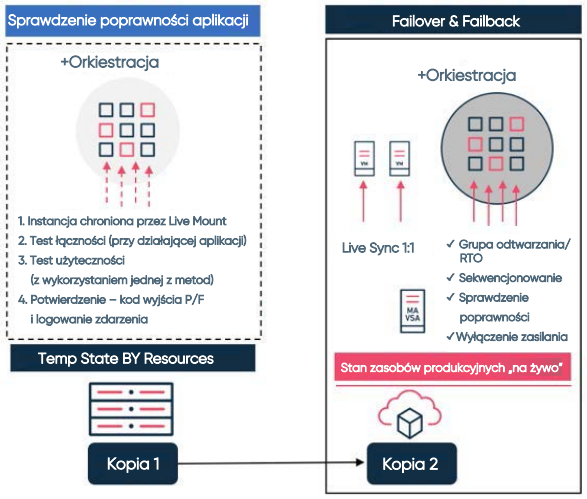


- **Integracja systemu zarządzania informacjami i zdarzeniami dotyczącymi bezpieczeństwa (SIEM)** – istniejące platformy monitorowania bezpieczeństwa można wykorzystać w celu centralnego koordynowania działań i zdarzeń w środowisku systemowego, wtyczek lub interfejsów API można bezpiecznie eksportować zapis kontrolny, informacje o zdarzeniach, alerty i dzienniki do systemu SIEM lub na platformę SOAR w celu ich zachowania oraz na potrzeby orkiestracji zdarzeń.
- **Blokada oparta na uwierzytelnianiu certyfikatów** – gdy funkcja ta jest włączona, nie można dodać Klienta do architektury ochrony danych bez wykonania dodatkowych czynności administracyjnych i posiadania odpowiednich uprawnień.
- **Wysyłanie alertów** – alerty powiadamiające użytkowników o różnych zdarzeniach mogą być wysyłane automatycznie. Można również wbudować odpowiedni przepływ działań w procedurę wysyłania alertów, aby była ona uruchamiana przez administratora.

Łatwe osiąganie stanu gotowości do odzyskiwania danych

Kompleksowy plan ciągłej gotowości do odzyskiwania danych zapewnia poczucie bezpieczeństwa. W sytuacji zagrożenia poważnymi atakami nie ma nic gorszego, niż ciągłe zastanawianie się nad tym, które dane należy odzyskać w jakiej kolejności. Gotowość do odzyskiwania danych oznacza, że kolejne etapy tego procesu są udokumentowane, zautomatyzowane i przewidywalne. Commvault zapewnia następujące możliwości zwiększające gotowość do odzyskiwania danych:

- **Architektura ochrony danych o wysokiej dostępności** – architektura Commvault może być chroniona za pomocą replikacji bazy danych za pomocą funkcji Live Sync do jednego lub więcej węzłów zapasowych. Ochrona bazy danych jest możliwa wewnętrznie w chmurze publicznej. Commvault zapewnia tę usługę bezpłatnie.
- **Koordynacja odzyskiwania danych** – Commvault zapewnia platformę sterowania, która obsługuje i utrzymuje rekordy wszystkich zgromadzonych danych oraz zarządza nimi. Do odzyskania tych danych wystarczy jedno kliknięcie. Procedurę można przetestować, przeprowadzając w pełni skoordynowane próbne przełączenie awaryjne i odtworzenie danych bez przerywania procesów produkcyjnych.
- **Sprawdzanie integralności danych** – Commvault udostępnia różne metody sprawdzania integralności danych. W odniesieniu do danych przesyłanych, przyjmowanych i zapisywanych na nośnikach pamięci masowej stosowane są sygnatury. Ponadto w regularnym sprawdzaniu integralności danych na nośnikach pamięci masowej pomagają zadania zautomatyzowane.



- **Sprawdzanie odtwarzalności aplikacji** – ta w pełni skoordynowana procedura umożliwia dostęp do kopii bezpieczeństwa danych bezpośrednio z infrastruktury tworzenia kopii zapasowych, uruchomienie aplikacji, nawiązanie połączenia oraz przeprowadzenie testu sprawdzającego odtwarzalność zarówno danych, jak i aplikacji.
- **Łatwe określanie danych do odtworzenia** – można przeszukiwać dane z dowolnego okresu, wykorzystując takie opcje, jak pokaż/ukryj elementy usunięte, ostatnie, dotyczące konkretnego punktu lub przedziału czasowego. Opcje te ułatwiają wybór danych do odtworzenia.

Certyfikaty branżowe

Rozwiązanie Commvault do ochrony danych ma certyfikaty zgodności z następującymi normami (jeśli procedura certyfikacyjna jest w toku, zostało to zaznaczone):

- **Common Criteria** – w toku
- **FedRAMP** – status „High Ready" w programie Federal Risk and Authorization Management Program (FedRAMP) dla produktów Metallic Backup as-a-Service (BaaS) i Metallic Cloud Storage Service (MCSS)
- **FIPS 140-2** – program sprawdzania poprawności modułu kryptograficznego (Cryptographic Module Validation Program)
- **Zgodność z normą NIST 800-53 CP9** – specjalna publikacja NIST 800-53 (Rev. 4) CP-9
- **Zgodność z normą NIST 800-53 CP10** – specjalna publikacja NIST 800-53 (Rev. 4) CP-10
- **STIG (Security Technical Implementation Guide)** – certyfikat dla rozwiązania Commvault HyperScale™ Storage Pool
  - Certyfikat STIG – wyniki skanowania dostępne pod adresem at https://documentation.commvault.com
- **VPAT 2.0 – zgodność z normami WCAG i 508** – deklaracja VPAT 2.0

Ochrona przed atakami typu ransomware ma ogromne znaczenie dla Twojej firmy i kariery. Jej brak może spowodować utratę danych, przychodów i wiarygodności. Skuteczna ochrona sprawia natomiast, że nawet w przypadku takiego ataku jego skutki są usuwane szybko, dzięki czemu firma i użytkownicy nie muszą się obawiać o wyniki swojej pracy. Możesz sobie ją zapewnić już dziś!

Dowiedz się więcej o rozwiązaniach chroniących przed atakami ransomware. Zapraszamy na stronę commvault.com/ransomware >