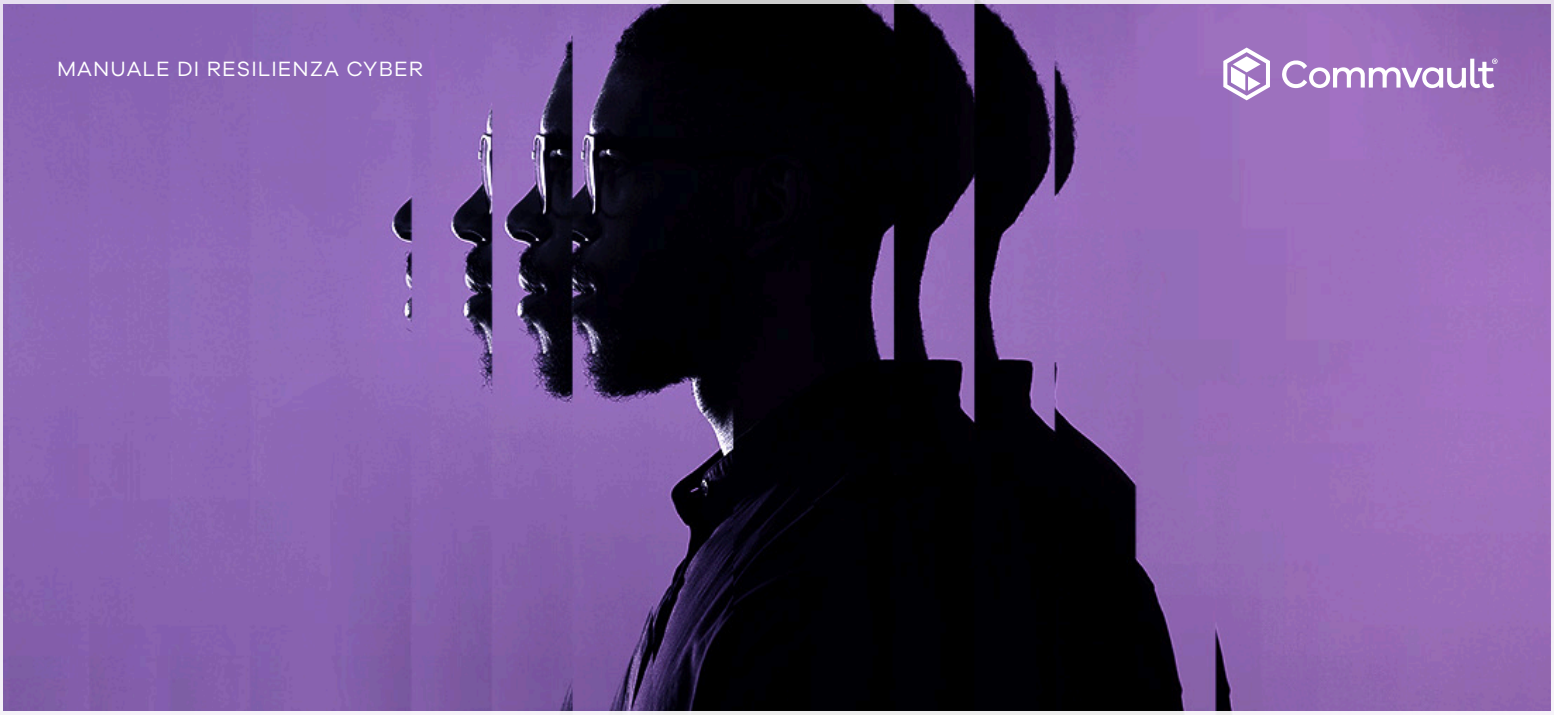
MANUALE DI RESILIENZA CYBER

Le migliori pratiche per passare dalla operatività minima (minimum availability) alla completa ripresa cyber

Commvault®



INTRODUZIONE

Essere preparati per la ripresa cyber è fondamentale nell'era digitale odierna, dove le minacce cyber sono sempre più sofisticate e diffuse.

Strategie di ripresa cyber efficaci sono essenziali per contrastare queste minacce e permettere alla tua azienda di ripristinare rapidamente i sistemi e i dati critici dopo un incidente cyber – minimizzando il tempo di inattività e mitigando l'impatto sulle operazioni aziendali. Essere pronti al cyber rischio dimostra ai clienti, agli stakeholder e agli enti regolatori che l'azienda è seria nel proteggere i dati sensibili e i sistemi che garantiscono il rispetto degli impegni verso i clienti.

Il primo passo per costruire un piano di prontezza cyber è identificare le persone, i processi, i sistemi e i dati critici necessari per operare – questa è la tua **operatività minima (minimum availability)**. Per la maggior parte delle aziende, questo include la gestione esecutiva e operativa, una comprensione dei ruoli e delle responsabilità durante il ripristino, nonché la capacità tecnica di ripristinare i sistemi critici, come l'identità aziendale (ad esempio, Active Directory), i canali di comunicazione (ad esempio, email, chat, strumenti di collaborazione) e di preparare e validare che dati, applicazioni e infrastrutture siano puliti e pronti per essere ripristinati da backup.

Oltre alle normative di conformità (come GDPR, HIPAA, DORA o SOCI) che richiedono piani dettagliati di cybersecurity, resilienza, ripristino di disastri e continuità aziendale, un piano di ripresa cyber ben strutturato riduce il rischio di perdita di dati, garantendo che informazioni critiche come dettagli dei clienti, dati proprietari e proprietà intellettuale rimangano protette. In caso di compromissione dei dati, avere un meccanismo di ripristino rapido aiuta a ristabilire rapidamentele operazioni minime e a riportare i sistemi online velocemente.

IL RAPPORTO DI COMMVAULT + GIGAOM SOTTOLINEA LA NECESSITÀ CRITICA DI STRATEGIE DI RIPRESA CYBER COMPLETE.

Continua a leggere per scoprire i componenti fondamentali necessari per essere pronti a un attacco cyber – e vedi come Commvault® Cloud fornisce gli strumenti per aiutarti a riuscire.

PASSO #01

IDENTIFICA

Un principio chiave di qualsiasi strategia è una visibilità approfondita dell'ambiente e una comprensione di quali applicazioni, sistemi e dati siano necessari per garantire l'operatività minima (minimum availability) in caso di interruzioni e attacchi cyber.

Con Commvault Cloud, ciò include la capacità di scoprire, classificare e monitorare i dati sensibili in tutti i tuoi archivi di dati. La classificazione dei dati può poi attivare politiche di protezione e aiutare le organizzazioni a identificare ciò che è più critico e ciò che richiede un livello di protezione diverso.

Una volta identificati gli elementi che devono essere protetti, puoi dotare l'ambiente di meccanismi di rilevamento delle minacce, rilevamento delle anomalie e sistemi di early alert per avvisare le squadre di sicurezza delle minacce nelle tue reti prima che causino danni.

Hai anche bisogno di un approccio a più livelli quando si tratta di individuare e bloccare malware, ransomware e altri vettori di corruzione dei dati. I dati devono essere ispezionati in tutti i punti del loro ciclo di vita per individuare i dati corrotti e poterli ripristinare a un punto pulito nel tempo.

PRODOTTI COMMVAULT CLOUD PER IDENTIFICARE LE MINACCE:

- Risk Analysis per la scoperta e il controllo dei dati sensibili
- Threatwise™ per il rilevamento delle minacce e delle anomalie e gli avvisi precoci
- Threat Scan per identificare dati maliziosi o corrotti

CAPACITÀ DELLA PIATTAFORMA COMMVAULT CLOUD:

- Cleanpoint Validation

PASSO #02

PROTEGGI

Per essere pronti a un attacco inevitabile, devi proteggere i tuoi dati dalle azioni dagli attaccanti, degli insider malintenzionati e persino dalle configurazioni errate o dalle interruzioni.

Questa protezione è molteplice e deve prendere in considerazione i dati stessi, l'identità e le configurazioni. Iniziando dai dati, la pratica migliore suggerisce che le organizzazioni seguano la regola 3-2-1: tre copie dei dati, su due tipi di supporto (o su due piattaforme diverse), e una copia che non può essere modificata. Duplicare i dati per i primi due passaggi è semplice, ma il terzo è un po' più complesso. Hai bisogno di un meccanismo che renda i dati immutabili e indelebili per proteggerli da modifiche o eliminazioni unilaterali.Questo è particolarmente importante per due ragioni: la maggior parte dei ransomware ha meccanismi per alterare i backup, e le minacce interne sono reali.

Devi anche verificare che la tua infrastruttura (sia cloud che di backup) sia configurata secondo i principi di zero trust. Dovrebbero esserci meccanismi in grado di controllare le configurazioni, segnalare e avvisare su eventuali cambiamenti o "drift." L'autenticazione dovrebbe seguire i principi di zero trust e includere l'autorizzazione multifattore e multipersona, a seconda dei livelli di accesso e delle azioni che vengono eseguite.

Inoltre, qualsiasi meccanismo tu abbia per la validazione dell'identità, come Active Directory o Entra ID, dovrebbe essere configurato, backuppato e monitorato per eventuali cambiamenti come aggiunte, eliminazioni o elevazioni di privilegi. Qualsiasi piano di dati, configurazione o controllo dovrebbe essere backuppato per consentire il ripristino in caso di incidente, e i backup dovrebbero essere isolati e separati dalla rete (air-gapped) per ridurre la probabilità che gli attaccanti li trovino durante la ricognizione o li eliminino o crittografino con malware o ransomware.

PRODOTTI COMMVAULT CLOUD PERPROTEGGERE I TUOI DATI:

- Backup and Recovery percarichi di lavoro cloud,on-premises e SaaS
- Active Directory Backup and Recovery per proteggere Active Directory e Entra ID
- Air Gap Protect per un archiviazione immutabile, indelebile e disconnessa
- Threat Scan per identificare e isolare dati maliziosi o corrotti

CAPACITÀ DELLA PIATTAFORMA COMMVAULT CLOUD:

- Security IQ per la gestione della sicurezza del tuo ambiente di backup
- Controllo degli accessibasato sui ruoli (RBAC) e autorizzazione multipersona

PASSO #03

RISPONDI

Nessuna tecnologia sarà utile se usata in silos. Per questo motivo, Commvault Cloud si integra con software di gestione delle informazioni e degli eventi di sicurezza (SIEM) e piattaforme di orchestrazione, automazione e risoluzione della sicurezza (SOAR).

Questo consente lo scambio di informazioni tra Commvault Cloud e altri strumenti per rilevare meglio gli eventi di sicurezza, i problemi di integrità dei dati e le attività anomale.

Indipendentemente dall'utilizzo di strumenti usati, siano la piattaforma XSOAR di Palo Alto Networks, Splunk SIEM, Microsoft Sentinel o altro, il rilevamento delle minacce e delle anomalie da parte di Commvault Cloud è un potente alleato per sviluppare la capacità di resilienza informatica e potenziare la gestione degli incidenti.

Quando Commvault Cloud trova file sospetti o riceve un avviso di anomalia da un'integrazione, quel file può essere automaticamente isolato dai tuoi dati di produzione e una copia inviata a una Sandbox per l'analisi, per determinare se è malizioso.

CAPACITÀ DELLA PIATTAFORMA COMMVAULT CLOUD CHE TI AIUTANO A RISPONDERE PIÙ RAPIDAMENTE ALLE MINACCE:

- Security ecosystem integrations, incluse le tecnologie SIEM e SOAR
- Threat intelligence integrations per una copertura più ampia delle minacce
- Sandbox integrations per consentire l'ispezione e l'esecuzione di file sospetti

PASSO #04

RIPRISTINA

Quando è il momento di ripristinare i dati, sia da un disastro che da un cyberattacco, hai bisogno di un piano che sia stato sperimentato e documentato; dati puliti e completi; flessibilità dei target di ripristino; la capacità di ripristinare tutto, dai dati all'applicazione che li utilizza; e *velocità*.

Il peggior momento per rendersi conto che il tuo piano di ripristino non funzionerà è quando sei di fronte a un attacco. Condurre test regolari sia di pianificazione minima che di ripristino completo è fondamentale per sapere che puoi ripristinare quando necessario, e aiuta i team che eseguono il ripristino a conoscere ciò che è loro richiesto. Questi test o esercitazioni del processo di ripristino dovrebbero verificare l'integrità dei dati e essere in grado di ripristinarli e ricostruire le applicazioni in un nuovo ambiente.

La portabilità è importante per i test e il ripristino, poiché un attacco o un'interruzione potrebbe richiederti di spostare interi carichi di lavoro in un nuovo e diverso ambiente. Questo potrebbe significare semplicemente cambiare account o potrebbe essere così drastico da spostarsi da un ambiente on-premises al cloud, o a un cloud diverso – quindi il tuo ripristino deve essere ibrido e flessibile.

Abbiamo già discusso della necessità di scansionare e monitorare i dati per anomalie, malware e altri difetti. Quando è il momento di ripristinare, è importante fare un'ultima verifica dei dati per confermare che siano puliti, pronti per il ripristino e non rischino di reinfettare il tuo ambiente.

Infine, dopo il ripristino, avrai bisogno di mantenere una copia dei dati e dei sistemi colpiti dall'attacco per fornirla ai team di investigazione, alle forze dell'ordine, agli assicuratori cyber o ad altre parti interessate. Questa copia forense dovrebbe essere mantenuta separata dal tuo ambiente di produzione e preservata così com'è per le tue indagini. Questo può aiutare la reverse-engineering del malware, a identificare l'attaccante e a identificare tecniche e procedure per essere pronti a contrastarne in futuro.

PRODOTTI COMMVAULT CLOUD CHE TI AIUTANO A RIPRISTINARE:

- Cleanroom Recovery per il test, la validazione e l'analisi forense del ripristino
- Threat Scan per verificare che i file da ripristinare siano puliti e privi di malware, ransomware e corruzione
- Cloud Rewind per ricostruire le applicazioni in diversi cloud, dal codice ai dati
- Active Directory Recovery per la continuità dell'identità anche in caso di cyberattacco

CAPACITÀ DELLA PIATTAFORMA COMMVAULT CLOUD:

- Cloudburst Recovery per un ripristino rapido e su scala in cloud, disponibile quando ne hai bisogno
- Cleanpoint Validation per fornire un punto temporale noto e pulito a cui ripristinare

PASSO #05

MONITORA

L'efficacia della pianificazione e della preparazione dipende dalla presenza di strumenti che possano avvisare i team di sicurezza e IT su eventuali anomalie o eventi nell'infrastruttura.

Monitorare le minacce che hanno infiltrato la tua organizzazione e che cercano di eludere la rilevazione è fondamentale per minimizzare il danno che possono causare. Più in fretta ne vieni a conoscenza, prima puoi rimuoverle e ripristinare i dati colpiti.

La sfida del monitoraggio è che molti strumenti di cybersecurity scatenano centinaia o migliaia di allarmi, creando molto rumore a causa dei falsi positivi. Questo porta le squadre di sicurezza a indagare su piste che non portano da nessuna parte, causando esaurimento e stanchezza – e sottraendo tempo alle indagini su minacce reali. Regolare i sistemi in modo che avvisino solo per attacchi veri è cruciale per aiutare le squadre a concentrarsi e trovare le vere minacce.

I dati di produzione e di backup dovrebbero essere monitorati costantemente per cambiamenti, anomalie e malware, per aiutare a individuare le minacce più rapidamente, minimizzare il rischio di ulteriori infezioni e ripristinare a dati noti e puliti. Questo include la capacità di analizzare i comportamenti dei file, non solo il contenuto, in modo da poter rilevare attacchi mai visti prima.

Puoi anche trarre beneficio dal consolidamento di tutto il monitoraggio in una singola piattaforma – in gran parte dei casi, uno strumento SIEM o SOAR che è monitorato costantemente dal personale di sicurezza e utilizzato per coordinare le indagini e la risposta.

PRODOTTI COMMVAULT CLOUD CHE ABILITANO IL MONITORAGGIO CONTINUO:

- Threatwise™ per individuare soggetti che stanno compiendo azioni di spionaggio e insidie, e per ricevere segnali precisi di un'eventuale violazione.
- Threat Scan per lo scanning continuo dei dati di backup e dei file
- Threat Scan Predict per scoprire attacchi zero-day o guidati dall'AI polimorfa

CAPACITÀ DELLA PIATTAFORMA COMMVAULT CLOUD:

- Security ecosystem integrations per aggiungere livelli ancora maggiori di intelligenza sulle minacce da provider terze parti

RIEPILOGO

In sintesi, è necessario essere consapevoli dei rischi che i tuoi dati presentano per la tua organizzazione.

01

Identifica ciò che è necessario per l'operatività minima (minimum viability) – i sistemi, le app e i dati critici per il funzionamento del tuo business.

02

Investi in strumenti avanzati di protezione, rilevamento e monitoraggio per migliorare la capacità della tua organizzazione di rilevare e rispondere rapidamente alle minacce cyber.

03

Sviluppa e mantieni un piano di risposta agli incidenti aggiornato, che assegni ruoli, responsabilità e procedure da seguire in caso di violazione.

04

Esegui test completi per essere in grado di coprire più scenari e di ripristinare completamente.

05

Monitora i tuoi sistemi e i backup in modo da avere la certezza che siano puliti e pronti quando necessari.

Per vedere come Commvault Cloud può aiutarti con la parte tecnologica del puzzle della cyber readiness, **richiedi una demo e una consulenza** ai nostri esperti di readiness e ripristino.