COMMVAULT

WHITEPAPER

Proteggi i tuoi dati, il tuo ripristino e la tua mission

Il software di gestione e protezione dei dati deve condividere la tua mission con una tecnologia collaudata, una vigilanza costante, aggiornamenti e indicazioni.

Quando si parla di minacce informatiche, compresi i ransomware, il punto non è se, ma quando avverranno. Per assicurarti di poter recuperare i tuoi dati e non pagare il riscatto, devi essere certo che il tuo fornitore di servizi di protezione dei dati condivida il tuo livello di vigilanza. La soluzione giusta richiede la migliore tecnologia, le persone e i processi adatti.

Noi di Commvault, proprio come un CISO, operiamo in un costante stato di allerta. Con i prodotti e i servizi che forniamo, siamo molto reattivi nei confronti dei nostri clienti. Commvault ha guadagnato una solida reputazione come partner presente e fidato; i nostri molti clienti possono testimoniare la nostra reattività, innovazione e rapidità di esecuzione in contesti ad alta esposizione e ad alto impatto in caso di attacco ransomware.

La sicurezza dei dati è un obiettivo strategico per Commvault e viene perseguito attraverso la nostra protezione multilivello, il rilevamento avanzato e il ripristino rapido dalle minacce alla sicurezza, compresi i ransomware e le violazioni dei dati.

Le aziende hanno bisogno di strumenti per misurare costantemente la loro recovery readiness e di una strategia Zero Loss per limitare gli impatti di un attacco ransomware.

Quando si pensa alle minacce che interessano i dati di backup, un approccio comune è quello di creare copie con un certo livello di isolamento, come le copie air-gapped e non modificabili. Commvault sostiene questo approccio ed è esperta nel fornire sistemi di protezione non modificabili, separazione geografica e funzionalità di air-gap per le destinazioni di archiviazione on-premise e nel cloud, con la possibilità di utilizzare le nostre appliance o il tuo archivio.

Garantire la sicurezza dei dati e allo stesso tempo permettere al software di essere amministrato efficacemente può essere una sfida per molti. Commvault è all'avanguardia nel mettere in sicurezza i dati e nel fornire protezione rispetto a questioni come la privacy, il furto, la corruzione e la cancellazione, sia da minacce interne che esterne, deliberate o meno.

L'AAA Security Framework for Authentication, Authorization, and Accounting è uno strumento prezioso per valutare qualsiasi soluzione software ed è ben noto all'interno degli operatori della sicurezza. Commvault lo usa per valutare, migliorare e mostrare le sue funzionalità e l'aderenza ai regolamenti e alle best practice del settore. Aderendo ai principi di zero-trust zero come delineato dal NIST SP 800-207, Commvault fornisce ai clienti la gamma di servizi necessari per segmentare/isolare i dati, stabilire l'identità dell'utente, fornire l'accesso con il minimo privilegio richiesto, tutelarsi dagli errori dell'utente e avere una capacità di registrazione e auditing granulare completa. Questi controlli funzionano tramite tutti i tipi di accesso, UI, riga di comando o API.

Le minacce non sono sempre di origine esterna, il risultato di credenziali compromesse o di atti deliberati di soggetti malintenzionati. Per combattere le minacce interne, Commvault ha implementato un meccanismo di controllo a garanzia che le attività amministrative che potrebbero costituire una minaccia per i dati siano approvate da due o più amministratori con privilegi dedicati, applicando il principio "dei quattro occhi" alla sicurezza dei dati.

Una soluzione di ripristino è adeguata solo se è resiliente. Ad esempio, nel caso di un ripristino dei dati che richieda di tornare alla situazione precedente alla corruzione. Un altro esempio è il ripristino completo delle applicazioni aziendali in una nuova sede. Progettare la recuperabilità attraverso gli ambienti e fornire un'automazione semplificata per testare e verificare ogni scenario aiuta a raggiungere la recovery readiness. Sapere che i dati e le applicazioni critiche sono già stati testati per il ripristino da un processo automatizzato garantisce il livello di sicurezza, conformità e serenità necessario.

Commvault ha sviluppato dei metodi per integrare il software di sicurezza con funzionalità di monitoraggio e rilevamento con gli aspetti critici di una data architettura di protezione dei dati. Gli algoritmi di apprendimento automatico rilevano le anomalie nell'attività dei file, e l'implementazione di file honeypot fornisce un campanello d'allarme precoce sui potenziali attacchi ransomware. Questi strumenti forniscono ulteriori funzionalità di messa in allerta precoce senza aumentare i costi o lo sforzo di gestione.

Il grafico qui sotto riassume le principali minacce e come possono essere affrontate con Commvault.

Minaccia	Strategia
I dati di backup sono presi di mira dai ransomware	Proteggi i backup, rendendoli non modificabili da qualsiasi account amministratore. Le modifiche possono essere effettuate solo per i processi Commvault verificati. Un'ulteriore sicurezza è fornita dalla firma digitale e dalla richiesta di autenticazione del certificato tra le componenti Commvault.
Gli attacchi prendono di mira password, policy e dati	Autenticazione sicura con una scelta di controlli multi-fattore, con blocco degli accessi granulare, basato sui ruoli all'interno dell'azienda in funzione delle responsabilità e degli ambiti di competenza. I dati sono criptati e hanno un supporto esterno per la gestione delle chiavi. Il principio del flusso di lavoro "a quattro occhi" protegge dalle attività di amministrazione potenzialmente distruttive.
Accesso amministratore ai dati di backup da parte di malintenzionati	Oltre al principio "dei quattro occhi" e al limite rappresentato da un blocco granulare basato sui ruoli, ogni accesso e modifica saranno registrati, e qualsiasi cambiamento critico sarà segnalato a un sistema a scelta. L'opzione di blocco della privacy protegge i dati sensibili e privati assicurando che non possano essere visti o ripristinati da un amministratore.
Cancellazione accidentale da parte dell'amministratore	Verranno applicati anche tutti i controlli che tengono fuori minacce e amministratori disonesti, rimuovendo così il potenziale di errore da parte degli amministratori.
Rispettare le implicazioni e le normative di sicurezza per la gestione dei file di log	Le aziende devono stabilire delle policy per garantire la conformità con le leggi e i regolamenti a cui sono soggette, in genere conservando i registri per periodi prolungati. I file di log da server, endpoint e dispositivi di rete possono essere conservati indipendentemente dalla normale policy di conservazione dei backup.

Questa guida offre una raccolta di best practice fondamentali per la sicurezza impiegate dalla nostra rete di clienti globale. Queste pratiche sono state adattate attraverso un processo di continuo miglioramento e innovazione per garantire la sicurezza dei dati e la recovery readiness, seguendo l'aumento costante del volume dei dati e il panorama che si espande oltre i sistemi di archiviazione aperti, fino al cloud.

Raccomandazioni sulla sicurezza dei dati

La sicurezza dei dati aiuta le aziende a proteggersi e recuperare i dati derivanti da minacce alla sicurezza, comprese le violazioni dei dati e i ransomware, controllando al contempo l'accesso ai dati chiave. Gli Intelligent Data Services di Commvault includono il rilevamento avanzato delle minacce e delle anomalie, parte di una funzionalità di protezione multilivello che aiuta a mitigare l'impatto delle minacce sui tuoi dati. Gli attacchi ransomware fanno notizia, e con Commvault è possibile ridurre il rischio che se ne verifichi uno e contribuire ad accelerare il ripristino in caso di attacco.

Security Health Assessment Dashboard

Il punto di partenza è identificare e valutare correttamente i rischi e le lacune. Il Security Health Assessment Dashboard è disponibile sia in Commvault Cloud Metrics Reporting che in Commvault Command Center™. Il Security Health Assessment Dashboard fornisce rapidamente approfondimenti e raccomandazioni per costruire un piano d'azione. Tutti i controlli e le impostazioni consigliati possono essere trovati in questa dashboard e implementati rapidamente tramite azioni interattive. Per ulteriori informazioni, consulta Migliorare la gestione del rischio con Commvault Security Health Assessment Dashboard.

Strategia Zero Loss

Ridurre i rischi di un attacco ransomware è sfidante, ma definire una strategia in grado di offrire visibilità sui tuoi dati e abilità di fare un immediato recovery sono elementi fondamentali per ripristirare le operazioni di business. Tuttavia è necessario definire una strategia che sia in grado di pianificare, gestire e ridurre l'impatto del ransomware, oltre a gestire immediatamente il recovery in caso di attacco. Utilizzando una piattaforma di gestione centralizzata si riduce le complessità e si protegge ciò che di più prezioso si ha in azienda. Il tutto grazie ad una strategia Zero Loss.

Backup immutabili

Garantire che le copie di backup non siano modificabili e non possano essere alterate o criptate dai ransomware è fondamentale. Deve essere un processo conveniente per tutti i dati all'interno del tuo ambiente, che deve poter essere attivato per l'archivio che scegli tu: on-premise, nel cloud o soluzioni Commvault HyperScaleTM. È una scelta chiara con un beneficio maggiore rispetto alle soluzioni unicamente air-gap, ed elimina complessità e costi aggiuntivi.

La funzionalità che blocca le modifiche degli archivi di backup impiega metodi collaudati per limitare le operazioni di scrittura e di cancellazione, impedendo ai malintenzionati o ai malware di modificare i file nel percorso protetto. Commvault ha recentemente testato l'affidabilità e l'efficacia di questa funzionalità con la tecnica di bypass RIPlace, in grado di violare diverse soluzioni endpoint di sicurezza simili. Commvault, tuttavia, ha dimostrato di fornire una protezione sicura da RIPlace.

Noi raccomandiamo una strategia multilivello, e alcuni clienti scelgono di implementare tecniche aggiuntive per una maggiore protezione. Per dati specifici, le aziende possono utilizzare copie WORM on-premise o nel cloud, e implementare strategie di isolamento air-gap. In Commvault, si possono inserire facilmente attraverso le policy, compresa la segmentazione della rete, topologie di rete crittografate, gateway e firewall. Inoltre, le soluzioni Commvault supportano l'automazione per orchestrare la disconnessione dalla rete e dai server.

Rafforzamento della sicurezza

Il rafforzamento della sicurezza è essenziale per tutti gli ambienti software. I componenti principali della soluzione Commvault si basano sul sistema operativo, sul database, sull'applicazione e sulla tecnologia del server web sottostante. Quindi tutte le falle di sicurezza all'interno delle tecnologie sottostanti devono essere chiuse per non diventare punti di ingresso per le minacce informatiche.

- **Applicazione delle raccomandazioni di rafforzamento della sicurezza** – abilitazione automatica delle raccomandazioni basate sugli standard del National Institute of Standards and Technology (NIST).
- **Firma binaria che include le terze parti** – un framework Commvault per firmare digitalmente i binari e garantire che un malintenzionato non li abbia modificati. Tutte le librerie di terze parti vengono aggiornate regolarmente e in risposta alle vulnerabilità segnalate.
- **Rafforzamento CIS Level 1** – il software Commvault è stato testato e verificato CIS Level 1.

Rafforzamento delle applicazioni con autenticazione, autorizzazione e accounting

Il protocollo AAA è un quadro di sicurezza che permette di controllare in modo intelligente l'accesso alle risorse del computer, applicare le policy e verificare l'uso. Questi processi combinati sono considerati essenziali per un'efficace gestione e sicurezza della rete. Commvault offre una gamma di funzionalità sicure, solide e complete in ciascuna di queste tre aree.

COMMVAULT

WHITEPAPER

Quadro di sicurezza AAA per il controllo degli accessi

Autenticazione	Autorizzazione	Accounting
Verifica e concessione dell'accesso	Controlla quale livello di accesso viene richiesto	Rilevazione e auditing dell'accesso e delle competenze

Autenticazione

Il processo di autenticazione si basa sul fatto che ogni utente ha un unico insieme di criteri per ottenere l'accesso. Commvault abilita metodi di autenticazione a più fattori (MFA) per rendere altamente improbabile che un account utente valido possa essere imitato.

- **Secure Lightweight Directory Access Protocol (LDAP)** – supporta Activate Director e i server di identità LDAP generici.
- **Fornitori di identità esterni** – sono supportati utilizzando protocolli sicuri come Open Authorization (OAuth) e Security Assertion Markup Language (SAML).
- **Autenticazione a più fattori** – con login tramite applicazione authenticator, smart card e chiavi di autenticazione hardware.
- **Autenticazione della certificazione** – per proteggere l'infrastruttura Commvault dallo spoofing.
- **Multitenancy** – con micro-segmentazione amministrativa e compartimentazione degli accessi.
- **Gestione degli accessi privilegiati (PAM) con CyberArk** – archivia, organizza, protegge e gestisce centralmente le credenziali di Commvault, le credenziali degli account di servizio e le sessioni di accesso dell'amministratore senza esporre le password.

Autorizzazione

Dopo l'autenticazione, è necessario concedere l'autorizzazione all'utente per permettere di svolgere compiti specifici. Commvault fornisce un insieme ricco e completo di funzionalità:

- **Sicurezza basata sui ruoli** – gestisce le funzionalità assegnando ruoli a utenti e gruppi, incluso il supporto per ambienti multi-tenant, e limita l'accesso a server, applicazioni e set di dati.
- **Flussi di lavoro a doppia autorizzazione** – supporta il principio "dei quattro occhi" per attività amministrative come la cancellazione set di dati, client, ripristini, obiettivi, lavori e policy.
- **Passkey e blocco della privacy** – gli amministratori gestiscono i dati, ma non dovrebbero visualizzare o ripristinare i dati di cui non sono proprietari. Usando questi due strumenti insieme, solo il proprietario dei dati a livello individuale, di reparto o di azienda può ripristinarli con la passkey richiesta.
- **Crittografia dei dati** – crittografia certificata Federal Information Processing Standards (FIPS), codice a più di 6 cifre tra cui AES 256, dati criptati fin dall'inizio e per tutta la durata del processo di gestione.
- **Gestione delle chiavi di crittografia** – sistema di gestione delle chiavi (KMS) integrato o uso di un KMS esterno di terze parti, compreso qualsiasi sistema KMIP (Key Management Interoperability Protocol) compatibile, AWS KMS, Azure Key Vault e passphrase.
- **Crittografia di rete** – HTTPS, TLS 1.2, supporto Proxy/Gateway.
- **Third-party port mapping (TPPM)** – incanala le comunicazioni di terzi attraverso le porte di rete Commvault, riducendo drasticamente la complessità dell'implementazione in un ambiente sicuro.
- **Supporto per copie WORM** – le policy WORM, quando applicate alle copie di dati, fanno rispettare i diritti di rimozione e cancellazione e impongono una conservazione fissa dei dati.
- **Supporto del servizio Cloud WORM** – archiviazione a livello di bucket e di oggetto supportata per configurazioni WORM.

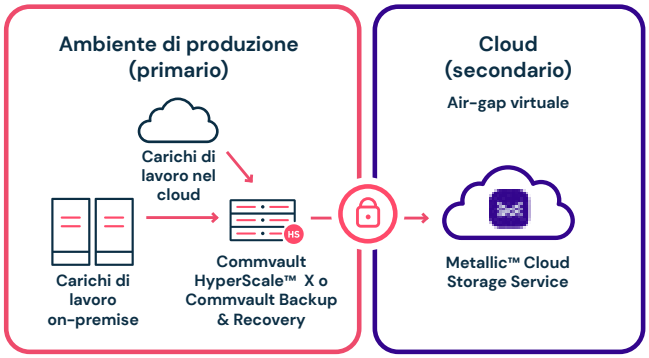
Accounting

L'accounting dovrebbe concentrarsi sulla registrazione completa degli accessi e delle azioni degli utenti dal punto di vista della sicurezza, garantendo l'osservabilità attraverso rapporti specifici e l'allerta al verificarsi di determinate condizioni. Le attività di accounting forniscono risposte a domande essenziali come:

- **Chi può accedere a troppi dati?** Il volume di accessi via UI, riga di comando e API è tracciato e riportato.
- **Cosa viene fatto con gli accessi?** Un intero audit trail degli accessi e delle azioni degli utenti.
- **Quali accessi possono essere revocati?** Il sistema segnalerà gli utenti che non hanno effettuato accessi in un determinato periodo di tempo per una possibile revoca.
- **Quali dati non sono criptati?** Un rapporto conferma lo stato della crittografia, come da raccomandazioni.

Isolamento dei dati e air-gap

"Air Gap" indica un'architettura di protezione dei dati che limita l'esposizione a un attacco e permette il ripristino dei dati a un momento precedente l'inizio dell'attacco. Commvault può affrontare efficacemente il rischio che i dati crittografati vengano copiati all'interno dell'architettura di backup con: destinazioni backup non modificabili, applicazione periodica di una policy di sicurezza WORM alle copie di dati e rimozione della funzionalità di cancellazione fino alla fine del periodo di conservazione. Commvault ha migliorato i controlli sugli accessi fisici disponibili per ogni soluzione, rafforzato la sicurezza, semplificato e ridotto i costi.



- **Orchestrazione air-gap** – automatizza i flussi di lavoro per orchestrare la disconnessione dalla rete e dal server.
- **Segmentazione della rete** – utilizza i controlli di sicurezza della rete per bloccare l'accesso alle destinazioni di archiviazione secondarie sia digitalmente che fisicamente.
- **Topologie di rete crittografate** – usa le policy di rete Commvault per isolare le comunicazioni e creare tunnel crittografati in uscita dalla destinazione di archiviazione isolata. I gateway Commvault possono controllare automaticamente le connessioni persistenti.
- **Passare facilmente a un'archiviazione su cloud sicura e scalabile** – Metallic™ Cloud Storage Service (MCSS) – è la "scorciatoia" verso un'archiviazione cloud sicura ed air-gapped delle copie secondarie, con costi prevedibili e nessuna infrastruttura richiesta.

Maggiore protezione dai ransomware con l'isolamento dei dati e le tecnologie air-gap **Leggi >**

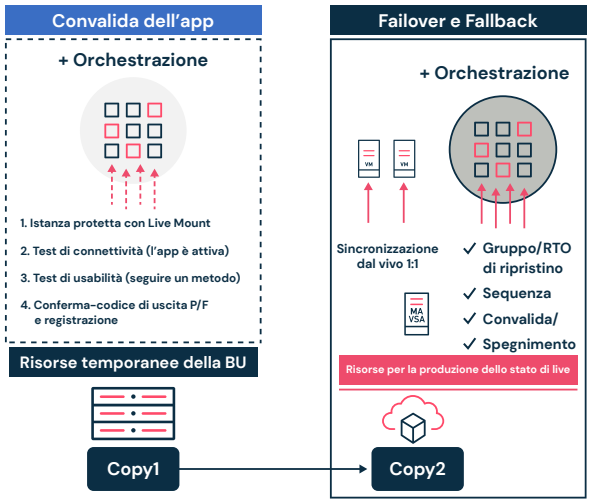
Monitoraggio e rilevamento

Molti esperti raccomandano di adottare una strategia anti-malware e ransomware a più livelli. Commvault ha incorporato queste funzionalità nel software di sicurezza e nelle policy esistenti per ottenere vantaggi più significativi senza il sovraccarico generato dalla gestione incrementale.

- **Monitoraggio dell'attività del file system** – utilizza dati storici e un algoritmo di apprendimento automatico per rilevare il comportamento del file system che si discosta dalle statistiche.
- **Monitoraggio dei file honeypot** – questi file nascosti, che sono comuni e attraenti per gli attacchi ransomware, vengono monitorati per rilevare i cambiamenti di firma.
- **Integrazione di Security Information and Event Management (SIEM)** – usa le piattaforme di monitoraggio della sicurezza esistenti per gestire e orchestrare azioni ed eventi Commvault a livello centrale. Attraverso Syslog, plugin o API, esporta audit trail, eventi, avvisi e log in modo sicuro nella tua piattaforma SIEM e SOAR per la conservazione e l'orchestrazione degli eventi.
- **Blocco dell'autenticazione dei certificati** – quando il blocco dei certificati è abilitato, i client non possono essere aggiunti all'architettura di protezione dei dati senza ulteriori passaggi amministrativi e privilegi.
- **Allarme attivabile** – agisce automaticamente e invia segnalazioni o incorpora un flusso di azioni raccomandate nell'alert all'amministratore.

Semplificazione della recovery readiness

La vera serenità nasce dall'avere un piano completo e continuo di recovery readiness. L'ultima cosa che serve quando si affronta un attacco è fermarsi per capire quali dati devono essere recuperati e n quale ordine. Recovery readiness significa che le fasi di recupero sono documentate, automatizzate e prevedibili. Le funzionalità di Commvault per supportare la recovery readiness includono:



- **Architettura di protezione dei dati ad alta disponibilità** – l'architettura Commvault può essere protetta utilizzando una replica Live Sync del database su uno o più nodi standby. Il database può essere protetto in modalità nativa in qualsiasi cloud pubblico, e questo è un servizio di protezione gratuito offerto da Commvault.
- **Orchestrazione del ripristino** – il piano di controllo di Commvault gestisce, opera e mantiene i record di tutti i dati raccolti. Può essere ripristinato completamente con un solo clic, cosa che può essere testata in anticipo con un failover di prova completamente orchestrato per assicurare un ripristino sicuro senza interrompere la produzione.
- **Convalida dell'integrità dei dati** – Commvault fornisce diversi metodi di convalida dell'integrità dei dati. Le firme dei dati vengono utilizzate per confermare l'integrità di qualsiasi dato trasferito, ricevuto e registrato sui supporti di memorizzazione. Inoltre, sono previste delle attività automatiche per convalidare regolarmente i dati in memoria.
- **Convalida della recuperabilità delle applicazioni** – un'attività di convalida della recuperabilità delle applicazioni completamente orchestrata può fornire l'accesso direttamente alla copia di protezione dei dati dall'infrastruttura di backup, avviare l'applicazione, connettersi ed eseguire un test per convalidare sia i dati che la recuperabilità delle applicazioni.
- **Identificazione facile dei dati da ripristinare** – i dati possono essere cercati in qualsiasi lasso temporale, e le opzioni applicate includono mostrare/nascondere gli elementi cancellati, gli ultimi dati, un punto specifico nel tempo e un lasso di tempo. Queste opzioni rappresentano un modo semplice per selezionare i dati giusti da ripristinare.

Certificazioni di settore

Le seguenti certificazioni di conformità vengono rilasciate (o sono in attesa, dove indicato) con la soluzione di protezione dei dati Commvault:

- **Certificazione Common Criteria** – In attesa
- **FedRAMP** – Stato "High Ready" del Federal Risk and Authorization Management Program (FedRAMP) per il portafoglio Metallic Backup as-a- Service (BaaS) e Metallic Cloud Storage Service (MCSS)
- **Certificato FIPS 140-2** – Programma di convalida del modulo crittografico
- **Conforme a NIST 800-53 CP9** – Edizione speciale NIST 800-53 (ver. 4) CP-9
- **Conforme a NIST 800-53 CP10** – Edizione speciale NIST 800-53 (ver. 4) CP-10
- **STIG (Security Technical Implementation Guide)** – Certificazione per Commvault HyperScale™ Storage Pool
  - **Certificazione STIG** – risultati disponibili su https://documentation.commvault.com
- **VPAT 2.0 - Conforme a WCAG e 508** – Dichiarazione VPAT 2.0

I rischi e i benefici rappresentati da un sistema di difesa dagli attacchi ransomware sono significativi per la tua azienda e la tua carriera. Un livello di sicurezza scadente si traduce nella perdita di dati, di entrate e di credibilità. Una buona protezione dagli attacchi può portare a un ripristino rapido ed efficace delle attività, e a un maggiore riconoscimento per un lavoro ben fatto. La scelta è tua, ed è semplice: sii recovery ready!

Scopri di più su come usare la protezione dei dati come scudo contro i ransomware. Visita **commvault.com/ransomware >**