Commvault

GUIDA ALL'ACQUISTO

Ransomware: allineamento dei piani di protezione e recovery con le funzionalità critiche

L'azienda in evoluzione e la minaccia del ransomware

Le aziende si trovano ad affrontare situazioni sempre più critiche per quanto riguarda l'ambiente dati, a causa di molteplici fattori che vanno dall'aumento dei posti di lavoro ibridi e remoti, alla crescente diffusione dei dati fino all'aumento delle minacce avanzate, con danni da cybercrime che si prevede raggiungeranno i 10,5 trilioni di dollari all'anno entro il 2025.[1] Per ottenere una vera resilienza informatica, in un mondo sempre più ibrido, le aziende hanno bisogno di soluzioni mirate, che vadano oltre i tradizionali backup e recovery. Queste soluzioni consentono alle aziende non solo di proteggere i propri dati, ma anche di anticipare in modo proattivo i rischi potenziali, di ridurre al minimo i danni e di riprendersi rapidamente di fronte alle avversità. Questo aiuta le organizzazioni a ridurre l'esposizione complessiva al rischio e a gestire efficacemente i costi.

$10,5 TRILIONI
all'anno entro il 2025.[1]

È chiaro che i vecchi metodi non sono più efficaci. Le aziende si stanno orientando verso una nuova generazione di sicurezza dei dati basata su framework multilivello che forniscono difese attive e automazione, offrendo il miglior piano di protezione e recovery dagli attacchi ransomware.

SCOPO DI QUESTA GUIDA

Utilizza questa guida per mappare le tue attuali capacità di protezione e recovery da ransomware e determinare il modo migliore per ottimizzare il tuo piano di risposta, in ambienti ibridi, cloud o con carichi di lavoro SaaS.

1 Cybersecurity Ventures, Steven C. Morgan, Cybercrime to Cost The World 8 Trillion Annually In 2023, Ottobre 2022

Cybersecurity Framework del National Institute of Standards and Technology (NIST)

01 **IDENTIFICAZIONE:** sviluppare una comprensione organizzativa per gestire il rischio legato alla cybersecurity in riferimento a sistemi, persone, risorse, dati e funzionalità.

02 **PROTEZIONE:** garantire la fornitura di servizi critici attraverso lo sviluppo e l'attuazione delle opportune misure di protezione.

03 **MONITORAGGIO:** stabilire procedure continue per riconoscere il verificarsi di un evento di cybersecurity.

04 **RISPOSTA:** implementare attività appropriate per difendersi da un incidente di cybersecurity conosciuto.

05 **RECOVER:** sviluppare e implementare attività appropriate per mantenere i piani di resilienza e per ripristinare qualsiasi capacità o servizio che sia stato compromesso a causa di un incidente di cybersecurity.

Per rafforzare la resilienza della tua infrastruttura dati, l'attuale Framework di Cybersecurity del NIST V1.1 raccomanda cinque pilastri necessari affinché un programma di cybersecurity sia completo ed efficace.

Per gestire efficacemente il rischio di cybersecurity in un panorama in continua evoluzione, il NIST ha redatto una versione aggiornata del framework: CSF 2.0. Uscita all'inizio del 2024, questa versione aggiornata introduce un sesto pilastro, Govern, che riposiziona i componenti della governance all'interno dei cinque pilastri già esistenti ed insiste su quanto la cybersecurity sia uno dei maggiori fattori di rischio per le imprese.

In ogni sezione di questa guida viene spiegato perché ogni livello di sicurezza è essenziale e vengono esaminate le funzionalità chiave da incorporare nella tua soluzione di protezione e recovery da ransomware.

01 IDENTIFICAZIONE

In un mondo ibrido, sapere esattamente dove e come vengono utilizzati i dati critici non è una sfida da poco. Strumenti efficaci per la sicurezza dei dati dovrebbero fornire visibilità sull'intero ambiente dati per individuare meglio le aree di rischio ed eliminare i punti ciechi. Questi proteggono sia i dati che i backup con un'architettura zero-trust che include protocolli di sicurezza integrati per proteggere i dati, impedire accessi indesiderati e garantire la conformità di fronte alle minacce in continua evoluzione. In caso di attacco riuscito, l'osservabilità end-to-end aiuta le aziende a prendere decisioni migliori con riferimento ai dati prima, durante e dopo un cyber attacco.

INDIVIDUAZIONE COMPONENTI CHIAVE	REQUISITI DEL RANSOMWARE	FUNZIONALITÀ DI COMMVAULT
Approfondimenti sulla protezione dei dati	Analisi e identificazione automatica dei problemi, con azioni raccomandate per affrontare questioni relative alla sicurezza.	All'interno di Commvault® Cloud si troveranno, in tempo reale, avvisi, riepiloghi e raccomandazioni basati su intelligenza artificiale.
Assessment automatico della sicurezza	Utilizza strumenti interattivi per valutare rapidamente il livello di sicurezza e applicare raccomandazioni per migliorare la sicurezza.	Identifica automaticamente la causa del problema e la relativa soluzione sulla base dell'analisi storica.
Valutazione automatizzata dell'integrità di backup	Verifica che i backup siano integri.	Le metriche cloud e on-premise forniscono report regolari sullo stato.
Report e dashboard di gestione dei dati	Visualizza rapidamente lo stato di disponibilità del backup e del recovery. Report e dashboard personalizzati per elementi di interesse specifici.	Dashboard unificate e report espandibili garantiscono una pronta recovery, grazie a KPI dettagliati.
Auditing	Tieni traccia delle modifiche ai dati, incluso chi ha effettuato l'accesso e la data della modifica.	Controlla gli accessi di utenti e indirizzi IP specifici. Monitora tutte le modifiche alla configurazione e gli eventi di backup e recovery in audit trail dettagliati.
Threat Deception	Intercetta gli attacchi prima che raggiungano gli obiettivi stabiliti.	Threatwise™ fornisce strumenti differenziati per rilevare le minacce zero-day e non conosciute negli ambienti di produzione, aiutando i clienti a individuare le cyber minacce avanzate prima della compromissione dei dati.
Analisi dei rischi	Identifica e analizza i dati sensibili e a rischio per ridurre al minimo l'esposizione e l'esfiltrazione dei dati.	• Identifica, categorizza e classifica le informazioni sensibili, come i dati personali e finanziari, per dare priorità a determinate misure di sicurezza e ridurre l'esfiltrazione dei dati in caso di violazione. • Adotta misure proattive per garantire la conformità alle normative e risparmiare sui costi di archiviazione archiviando dati obsoleti (ROT). • Safe Search & Share sfrutta l'intelligenza artificiale per individuare rapidamente i dati sensibili e le relazioni all'interno di grandi set di dati, garantendo che solo le corrette informazioni vengano condivise con le giuste persone.
Threat Scan	Individua e analizza le anomalie dei file per assicurarti di recuperare i dati validi ed evitare la reinfezione da malware.	• Identifica le minacce malware per evitare la reinfezione durante il recovery. • Threat Scan analizza i dati di backup per individuare i file crittografati o danneggiati, assicurando agli utenti il rapido ripristino delle versioni attendibili dei propri dati. • Threat Scan Predict aggiunge una tecnologia di previsione AI in tempo reale per scoprire le minacce ransomware basate sull'AI.

02 PROTEZIONE

Grazie alla conoscenza del tuo ambiente dati, puoi iniziare a ridurre la superficie di attacco per limitare le potenziali minacce e prevenire una diffusione sistemica. Proteggiti dagli accessi indesiderati e dalle modifiche ai dati provenienti dall'interno e dall'esterno grazie all'architettura zero-trust. Puoi isolare e segmentare le reti, adottare l'air-gapping per isolare e proteggere le copie di backup e incorporare la Cyber Deception Technology per intercettare le minacce prima della perdita di dati, della crittografia e dell'esfiltrazione. Gli attacchi ransomware possono verificarsi quando le credenziali vengono compromesse o quando le credenziali di un utente consentono un accesso privilegiato a sistemi di cui non si dovrebbe poter disporre. Assicurati che siano attivi i protocolli di sicurezza standard di settore per crittografare e proteggere i dati e ridurre l'impatto di un attacco ransomware.

PROTEZIONE COMPONENTI CHIAVE	REQUISITI DEL RANSOMWARE	FUNZIONALITÀ DI COMMVAULT
Immutabilità	Mantieni i dati di backup al sicuro da modifiche non autorizzate.	• Protezione anti-ransomware per sistemi basati su Windows e Linux. • Applica i blocchi di archiviazione per on-premise e cloud; personalizzali per soddisfare le esigenze aziendali. • Abilita la tecnologia WORM (Write Once, Read Many) per evitare modifiche non autorizzate e la tecnologia cloud air-gapping per proteggere ulteriormente dalle minacce ransomware.
Rafforzamento delle infrastrutture	Riduci l'esposizione alle minacce sull'infrastruttura di backup.	Il software Commvault® è stato testato e valutato compatibile con il rafforzamento di livello 1 del Center for Internet Security (CIS). La conformità ai controlli di sicurezza CIS di livello 1 è disponibile come VM CIS pre-rafforzata (distribuita tramite OVA) o come dispositivo hardware fornito come HyperScale X™. Anche tutti i sottocomponenti, compresi CommServe, gli agenti multimediali e i nodi di accesso, possono essere rafforzarti al livello CIS 1.
Autenticazione e autorizzazione	Controlla chi ha accesso e a quale livello, aggiungendo più livelli di autorizzazione per garantire maggiore sicurezza.	• I controlli di accesso basati sui ruoli limitano l'utilizzo non autorizzato insieme agli IdP SAML (Security Assertion Markup Language) e OATH per fornire un ulteriore livello di sicurezza. • Integrazione con Active Directory e LDAP. • Controlli di autenticazione a più fattori e di autenticazione a più persone per i blocchi di conservazione e autorizzazione dei comandi per proteggere i dati da incidenti e prevenire azioni distruttive. • Integrazione con strumenti per la gestione degli accessi privilegiati e strumenti avanzati di gestione delle identità e degli accessi come CyberArk, Yubikey e la biometria per una maggiore autenticazione e garanzia degli utenti (AAL3). • Integrazione just-in-time con CyberArk per ridurre al minimo il rischio di credenziali archiviate. • Crittografia dei dati end-to-end che consente alle piattaforme esterne di key management di gestire e controllare le chiavi e l'autenticazione dei certificati, proteggendo dall'accesso da parte di malintenzionati. • Software WORM (blocco di ritenzione) • Multitenancy

02 PROTEZIONE

PROTEZIONE COMPONENTI CHIAVE	REQUISITI DEL RANSOMWARE	FUNZIONALITÀ DI COMMVAULT
Crittografia	Implementa standard di crittografia conformi alle linee guida del settore.	Standard e strumenti per gestire efficacemente le chiavi di crittografia per il backup e il ripristino in Commvault: • Modulo di crittografia Federal Information Processing Standards • Gestione integrata delle chiavi • Integrazione con la gestione delle chiavi di terze parti • Sistema di gestione delle chiavi con passphrase
Backup Catalog Protection	Garantisci una protezione immutabile in più aree, sia in copie locali on-premise che nel cloud.	• Forte protezione contro il ransomware per le copie locali. • Backup su Air Gap Protect o su cloud di terze parti.
Isolamento/ Air-gapping	Segmenta e isola i dati dalle reti esterne e assicura un rapido ripristino in caso di attacco.	• Air Gap Protect utilizza l'air-gapping per isolare e proteggere i dati sensibili. • Gli apparecchi HyperScale X sono dotati di controlli air-gap integrati. • Topologie di rete: utilizza una topologia unidirezionale o proxy.
Protezione di Active Directory	Crea la capacità di proteggere e ripristinare Active Directory, di eseguire il backup degli attributi degli oggetti e di eseguire backup completi, differenziali, incrementali e sintetici.	La piattaforma Commvault Cloud offre protezione Active Directory con air-gap on-premise e basata su cloud.
Strategia di backup 3-2-1	Crea una strategia di backup efficace che garantisca che i dati siano sempre disponibili. Disponi di almeno tre copie dei dati, di cui due locali ma in luoghi diversi e una copia fuori sede.	• Configura copie illimitate di dati on-premise o in più endpoint cloud. • Air Gap Protect offre la possibilità di abilitare l'archiviazione cloud con air-gap.
Threat Deception	Individua tempestivamente gli attacchi ransomware, prima della perdita di dati, della crittografia, dell'esfiltrazione o di potenziali danni.	• Copri la tua superficie distribuendo sensori di minaccia (false esche) in blocco. • Imita risorse critiche con sensori preconfigurati. • Emula risorse altamente specializzate e uniche per il tuo ambiente.
Controlli di sicurezza on-demand	Rispetta le norme e tieni sotto controllo i criteri di rotazione delle password che non influiscono sulla protezione dei backup.	Migliora il livello di sicurezza con il controllo zero-trust ed elimina le credenziali compromesse. L'integrazione con CyberArk consente di recuperare le credenziali just-in-time, compresa l'archiviazione e la gestione sicura delle credenziali all'interno di CyberArk.

03 MONITORAGGIO

Le aziende colpite da una minaccia alla sicurezza potrebbero non rendersi conto di essere state attaccate fino a quando non è troppo tardi e la violazione si diffonde oltre il loro controllo. Pertanto, garantire la disponibilità di strumenti adeguati per acquisire rapidamente informazioni su un evento di cybersecurity è essenziale per contenere un attacco ransomware prima che colpisca un'infrastruttura più ampia. Incorporando allarmi precoci e monitoraggio approfondito di nuova generazione, puoi far emergere e neutralizzare le minacce zero-day e interne per difendere i tuoi dati. Rileva, devia e segnala più tempestivamente le attività dannose per ridurre gli interventi di ripristino.

MONITORAGGIO COMPONENTI CHIAVE	REQUISITI DEL RANSOMWARE	FUNZIONALITÀ DI COMMVAULT
Monitoraggio della sicurezza con l'AI	Utilizza l'AI per monitorare i framework di anomalie che supportano i backup delle macchine virtuali e le applicazioni SaaS, fornendo visibilità granulare delle attività insolite sui file utilizzando un audit trail per individuare potenziali eventi di sicurezza.	Sfrutta il potenziale dell'AI per: • Ottenere un recovery pulito, veloce e sicuro riducendo i falsi positivi con AI/ML. • Monitorare i backup e analizzare eventi e comportamenti per verificarne lo stato riuscito, in sospeso o non riuscito. • Prevedere la futura conformità agli SLA con l'analisi dei trend dei backup. • Individuare le anomalie attraverso le modifiche alle caratteristiche dei file dovute a corruzione, crittografia o file dannosi in tempo reale e sui dati di backup. • Scoprire le nuove minacce ransomware zero-day e basate sull'AI.
Monitoraggio del sistema	Monitoraggio dei workload e delle infrastrutture critiche.	• Raccogli informazioni sulle principali risorse quali CPU, memoria, dischi, reti, flussi e lettura/scrittura. • Ottieni dettagli sugli accessi e sull'attività relativa ai file e inviali ai sistemi SIEM/SOAR per visibilità e rimedio.
Monitoraggio dei log	Cerca eventi di log specifici per monitorarne l'attività. Cerca un evento particolare tra tutti gli eventi di log indicizzati nella dashboard. Cerca gli eventi di log associati a un particolare client, file di log, modello o criterio di monitoraggio.	La piattaforma Commvault Cloud consente di monitorare le condizioni dei file di log e gli eventi Syslog e Windows in modo dettagliato.
Threat Awareness	Ottieni in modo proattivo informazioni immediate sulle minacce attive e latenti.	• Esponi i sensori solo ai soggetti malintenzionati; sono invisibili agli utenti e ai sistemi legittimi. • Ottieni informazioni critiche su attività e tattiche. • Elimina i falsi positivi e riduci la sensibilizzazione agli avvisi. • Attira i malintenzionati a utilizzare risorse false.
Honeypot e attività dei file in tempo reale	Monitora le risorse a rischio di ransomware e identifica i punti di ripristino puliti.	Monitora i file sospetti in tempo reale, per rilevare le minacce e proteggere i backup in modo da garantire un recovery pulito dei file ed evitare la reinfezione degli stessi.

03 MONITORAGGIO

MONITORAGGIO COMPONENTI CHIAVE	REQUISITI DEL RANSOMWARE	FUNZIONALITÀ DI COMMVAULT
Threat Awareness	Ottieni in modo proattivo informazioni immediate sulle minacce attive e latenti.	• Esponi i sensori solo ai soggetti malintenzionati; sono invisibili agli utenti e ai sistemi legittimi. • Ottieni informazioni critiche su attività e tattiche. • Elimina i falsi positivi e riduci la sensibilizzazione agli avvisi. • Attira i malintenzionati a utilizzare risorse false.
Monitoraggio della sicurezza con l'AI	Utilizza l'intelligenza artificiale per monitorare i framework anomali che supportano i backup delle macchine virtuali e altri workload, come le app SaaS.	• Ottieni informazioni dettagliate su quando i backup subiscono modifiche anomale per favorire un recovery pulito, veloce e sicuro. • Trova versioni pulite dei dati per favorire un recovery pulito, rapido e sicuro. • Riduci i falsi positivi con AI/ML.
Honeypot e attività dei file in tempo reale	Monitora le risorse a rischio di ransomware e identifica i punti di recovery puliti.	Monitora i file sospetti in tempo reale per rilevare le minacce e proteggere i backup per garantire un recovery pulito dei file ed evitare la reinfezione degli stessi.

04 RISPOSTA

Una volta rilevato il ransomware, la tua risposta deve essere immediata. Ottenere informazioni dettagliate attraverso strumenti di sicurezza e avvisi proattivi consente all'azienda di difendere i tuoi dati. Politiche documentate e un piano di risposta agli incidenti aiutano a stabilire le procedure successive da adottare. La risposta deve essere sia tecnica che aziendale e ogni stakeholder, in ciascuna delle rispettive aree, deve comprendere il proprio ruolo e le azioni da intraprendere. Il coordinamento e la comunicazione tra i vari team sono essenziali. La chiave è che i team di sicurezza facciano tutto il possibile per contenere e arrestare la diffusione, mettendo in atto gli strumenti adeguati per evitare qualsiasi potenziale reinfezione.

RISPOSTA COMPONENTI CHIAVE	REQUISITI DEL RANSOMWARE	FUNZIONALITÀ DI COMMVAULT
Integrazione di SIEM (Security Information and Event Management) e SOAR (Security Orchestration Automation and Response)	Si integra perfettamente con le piattaforme SIEM e SOAR esistenti per monitorare, gestire e orchestrare azioni ed eventi da una posizione centrale. Esporta audit trail ed eventi e accedi in modo sicuro alle tue piattaforme SIEM e SOAR per la conservazione e l'orchestrazione degli eventi. Con il monitoraggio in tempo reale, puoi rispondere rapidamente a qualsiasi minaccia rilevata e proteggere le risorse di backup con l'azione appropriata.	Le integrazioni di Commvault consentono l'interoperabilità con varie piattaforme di orchestrazione come Microsoft Sentinel, Palo Alto Networks XSOAR, Splunk e ServiceNow. Le nostre integrazioni forniscono: • Visibilità in tempo reale su eventi e incidenti di sicurezza. • Funzionalità avanzate di automazione e orchestrazione. • Riduzione dei tempi di risposta agli incidenti e degli interventi manuali. • Miglioramento della collaborazione interna e del livello di sicurezza generale.
Alert	Fornisci notifiche automatiche sulle operazioni, come i lavori non riusciti. Gli avvisi vengono visualizzati nella pagina Avvisi attivati e gli utenti definiti ricevono una notifica tramite e-mail.	Ricevi alert attivabili in varie forme: e-mail, SCOM (Systems Center Operations Manager), SNMP, webhook e così via.
Dashboard	Visualizza un'anteprima delle informazioni più importanti raccolte da tutti i computer CommServe dell'azienda, come la percentuale di SLA, l'utilizzo della capacità e gli avvisi di backup.	La piattaforma Commvault Cloud offre un modo unificato di visualizzare e gestire la tua resilienza informatica sia on-premise che SaaS. Fornisce dashboard sulla sicurezza, sulla capacità e sull'utilizzo a livello globale, con dashboard di valutazione dello stato della sicurezza e delle attività insolite che forniscono ulteriori approfondimenti.
Strumenti di orchestrazione	Crea flussi di lavoro orchestrati per rispondere rapidamente agli eventi ransomware. Possibilità di integrazione anche con fornitori di terze parti.	• Crea facilmente workflow per comandi pre/post-backup. • Workflow tramite interfaccia a riga di comando, API REST, moduli PowerShell e SDK Python. • Integrazione con Splunk, ServiceNow, Ansible o Terraform.
Risposta proattiva alle minacce	Difendi attivamente la recuperabilità dei dati avvisando la sicurezza nel momento in cui inizia l'attacco.	• I sensori di minaccia vengono distribuiti intorno a risorse preziose (come file server, database, macchine virtuali e così via) per creare esche all'interno degli ambienti. • Consiglia in modo intelligente il posizionamento dell'esca analizzando i workload nell'ambiente di backup. • Ricevi avvisi altamente accurati nel momento in cui inizia un attacco.

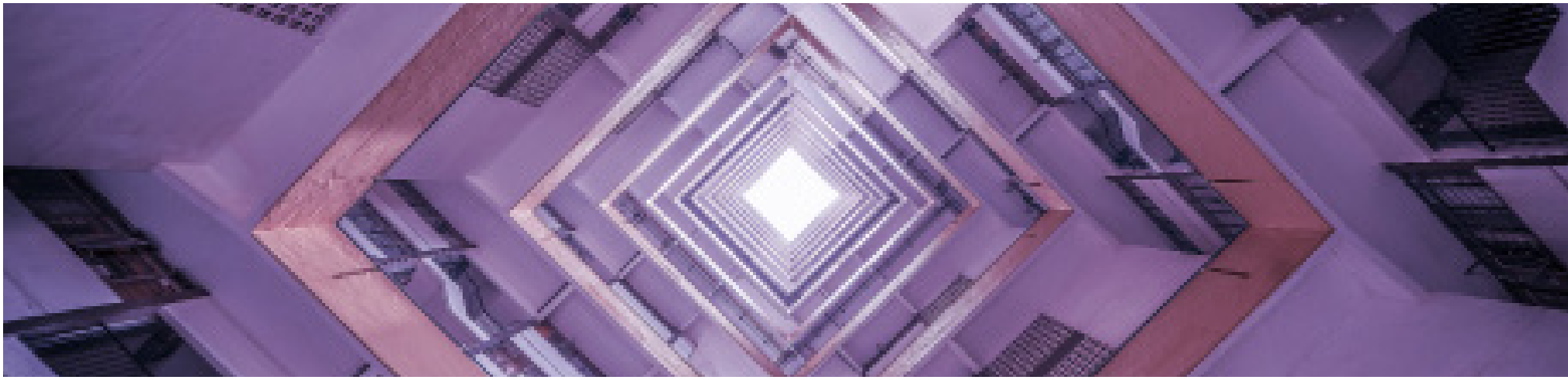
05 RIPRISTINO

Il processo di recovery inizia una volta identificate le minacce e dopo che una risposta adeguata agli incidenti isola e rimuove il malware. È fondamentale garantire che tutti i dati interessati vengano ripristinati alle normali condizioni operative del momento precedente all'incidente di sicurezza. È dimostrato che gli strumenti e le opzioni di recovery proattivi e affidabili per la più ampia copertura dei workload riducano i tempi di inattività, constrastino la perdita di dati e accelerino i tempi di risposta per una business continuity senza pari. Il piano di recovery inizia dopo che la causa principale è stata identificata e i file vengono ripristinati con l'obiettivo di avere strumenti di sicurezza futuri in grado di ridurre eventuali impatti. Durante le fasi di ripristino, è essenziale recuperare solo file puliti da tutte le tecnologie interessate.

RIPRISTINO COMPONENTI CHIAVE	REQUISITI DEL RANSOMWARE	FUNZIONALITÀ DI COMMVAULT
Ripristino multicloud ibrido	Recupera rapidamente i dati ovunque si trovino, sia on-premise che nel cloud.	Automatizza e ripristina su diversi hypervisor, hyperscaler o altre piattaforme.
High Availability	Con la funzione CommServe LiveSync, il server CommServe è pronto per il ripristino di emergenza e consente di eseguire rapidamente il failover su un host in standby designato in caso di disastro.	La funzionalità Commvault LiveSync consente il backup di cataloghi e workload critici.
Incident Response Recovery	Consenti ai team di incident response di recuperare in modo sicuro i dati per le indagini forensi.	• Organizza recovery out-of-place in una clean room isolata. • Esegui pre-/post-script e workflow per validare ed esaminare dati chiave.
Malware scanning	Verifica che i dati di backup siano recuperabili e che non vi siano minacce nel contenuto.	• Prepara in tempo reale le VMs utilizzando applicazioni di convalida per l'esecuzione in sicurezza degli script e la scansione delle stesse . • Esegui la scansione delle minacce prima che si diffondano con AI/ML, anomaly detection e scansione delle malware signature.
Curated Recovery e Sanitization	Riduci la perdita di dati grazie a un recovery coerente e ottimizzato, rimuovendo i file sospetti e conoscendo il momento esatto in cui effettuare il ripristino dei file integri.	Rimuovi, isola e metti in quarantena i file sospetti attraverso il rilevamento delle anomalie e sanifica il contenuto del backup esaminando e rimuovendo le minacce.
Proactive Recovery	Rileva e correggi le minacce prima che raggiungano l'obiettivo.	Con Threatwise™ inganni i malintenzionati, devi i loro attacchi verso risorse false, ottieni visibilità immediata sugli attacchi e rimedi tempestivi alle minacce, prima che raggiungano i tuoi dati.
Recovery Validation	Pianifica, implementa, convalida e dimostra di essere in grado di ripristinare.	• Convalida i backup in modo continuo o periodico per rilevare quelli danneggiati nelle prime fasi del ciclo. • Dimostra di essere in grado di effettuare il recovery senza interrompere le operazioni. • Riduci le complessità dei test di recovery eliminando i passaggi manuali.

05 RIPRISTINO

RIPRISTINO COMPONENTI CHIAVE	REQUISITI DEL RANSOMWARE	FUNZIONALITÀ DI COMMVAULT
Recovery Forensic	Esegui analisi forensi in modo sicuro in reti isolate senza causare ulteriori infezioni.	• Utilizza File Data Analysis per rilevare i file che potrebbero essere crittografati o danneggiati da malware per assicurarti di non eseguire il backup di file infetti. • Incorpora l'analisi delle minacce per rilevare i contenuti dannosi nei dati di backup al momento del ripristino per assicurarti di non rischiare una reinfezione dei sistemi di produzione durante il ripristino dall'ultimo momento temporale valido dei backup.
Recovery Orchestration	Disaster e cyber recovery orchestration con sistema di reporting sulla compliance automatizzato.	• Recovery one-click con copie pulite di diversi workload in produzione dopo validazione e sanificazione.
Rapid Infrastructure Recovery	Recovery rapido in cloud senza limitazioni sulle diverse location di ripristino dati.	• Combina test continui, infrastructure-as-code, scalabilità in cloud per automatizzare velocemente, in modo prevedibile e con alta affidabilità la cyber recovery dei workload ibridi, al più basso TCO. • Portabilità any-to-any che consente il ripristino da qualsiasi luogo in qualsiasi luogo.



Vera cyber resilience, con il TCO più basso.

Commvault Cloud offre una difesa su più livelli, minimizzando gli attacchi con early warning e cyber deception, grazie ad una soluzione completa di scansione delle minacce, remediation, quarantena intelligente, convalida del recovery pulito e velocità di recupero senza precedenti.

Implementa sin da oggi una strategia di cyber resilience con la soluzione migliore per aiutarti a prevedere, combattere proattivamente e accelerare il recovery dalle minacce informatiche.

Trova la soluzione migliore per le tue esigenze.

INTEGRAZIONI DI SICUREZZA COMMVAULT

Commvault offe integrazioni con i maggiori partner di sicurezza, per integrare le potenzialità della sua offerta e garantire diverse opzioni di cyber resilience in ambienti ibridi.

Scopri di più sulla cyber resilience
commvault.com/platform

Commvault®

commvault.com | 888.746.3849 | get-info@commvault.com