Rafforza il tuo piano di protezione dei dati con una soluzione Cyber Recovery più rapida e robusta

In base alla nostra ricerca, Dell Technologies PowerProtect Cyber Recovery offre l'isolamento fisico per i vault di backup e la scansione più approfondita per il ransomware

Isolamento air gap fisico per i vault di backup

Crea una barriera fisica che i dati non possono attraversare

Scansione più approfondita per il ransomware

CyberSense esamina i contenuti dei file e i database, non solo i metadati

Scansione dei carichi di lavoro anomali raddoppiata

Cerca i malware in più posizioni con un unico strumento

Il costo medio di un attacco ransomware è aumentato di quasi il 20% in due anni fino a raggiungere la cifra di 5,23 milioni di dollari[1]. Soluzioni efficienti di ripristino dagli attacchi informatici possono contribuire a ridurre o persino evitare questi potenziali costi, consentendo alle organizzazioni di eseguire rapidamente il ripristino in caso di incidenti, contenere la perdita di dati, ridurre al minimo i tempi di inattività e, nel frattempo, preservare l'integrità del marchio. Dopo un attacco, le soluzioni devono individuare e ripristinare i dati sicuramente validi, garantendo che l'organizzazione possa recuperare dati critici e sistemi e contribuendo al contempo a ridurre al minimo i rischi aziendali e i tempi di inattività.

Dell PowerProtect Cyber Recovery (Cyber Recovery) è una soluzione di questo tipo. Aiuta le organizzazioni a proteggere i dati e le applicazioni da ransomware, attacchi informatici distruttivi ed eventi imprevisti. Questo rapporto utilizza dati pubblicamente disponibili per mettere a confronto le caratteristiche di base della protezione dei dati e la funzionalità di Cyber Recovery e di una soluzione concorrente, Rubrik Security Cloud (RSC). Sono state esaminate in modo specifico le funzioni e la funzionalità che i clienti delle soluzioni di ripristino dagli attacchi informatici potrebbero ritenere importanti, tra cui vault di ripristino, immutabilità, carico di lavoro supportato, tecnologia di scansione, ripristinabilità e isolamento.

A differenza di RSC, Cyber Recovery utilizza un approccio multicopia, per cui, dopo la creazione dei backup, li copia (o, di solito, un sottoinsieme di backup selezionato) in uno storage isolato per la protezione e l'analisi. Cyber Recovery comprende diversi componenti, tra cui uno o più vault di storage, ubicati on-premise in un appliance PowerProtect Data Domain o nel cloud tramite la soluzione software-defined Dell APEX Protection Storage for Public Cloud. Al contrario, RSC non offre opzioni di vault locale. Cyber Recovery include anche CyberSense, un engine di analisi della sicurezza intelligente completamente automatizzato e integrato che analizza dati, file, database e immagini nel vault per individuare eventuali segni di danneggiamento dovuto a un attacco ransomware. La soluzione CyberSense è in grado di analizzare carichi di lavoro anomali due volte superiori rispetto alla soluzione Rubrik, differenza che consente alla funzione di ML (machine learning) con scansione di CyberSense di rilevare l'impatto di malware o altre attività dei responsabili delle minacce su più dati. Il diverso funzionamento di PowerProtect Cyber Recovery verrà analizzato in seguito e può rivelarsi più vantaggioso in base alle esigenze di ciascuna organizzazione.

Panoramica del prodotto

Panoramica di Dell PowerProtect Cyber Recovery

Dell PowerProtect Cyber Recovery comprende un appliance di storage che ospita i dati di produzione e un appliance di storage di destinazione nel vault per la replica. Comprende inoltre il software Cyber Recovery, che coordina la sincronizzazione, gestisce più copie di dati sul sistema PowerProtect Data Domain (PPDD) nel vault di Cyber Recovery e supervisiona il processo di ripristino nonché quello di analisi con CyberSense.

La soluzione trasferisce i dati univoci dall'MTree PPDD di produzione alla controparte del vault tramite la replica MTree e consente l'immutabilità dei dati* per una durata prestabilita. Il vault è dotato di un server che contiene il software Cyber Recovery e di un componente grazie a cui la soluzione ripristina le applicazioni e i dati di backup. Ogni vault di Cyber Recovery ospita in genere molti di questi componenti. Il vault contiene inoltre un host di analisi/indicizzazione dotato di software di analisi dei dati, che fornisce l'integrazione diretta tra il software Cyber Recovery e CyberSense.

*I prodotti Dell sono concepiti per supportare le iniziative dei clienti volte a proteggere i propri dati critici. Come qualsiasi prodotto elettronico, anche quelli per la protezione dei dati, lo storage e altri dedicati all'infrastruttura possono essere soggetti a vulnerabilità di sicurezza. È importante che i clienti installino gli aggiornamenti di sicurezza non appena vengono resi disponibili da Dell.

La Figura 1 fornisce una panoramica della soluzione Dell Cyber Recovery.

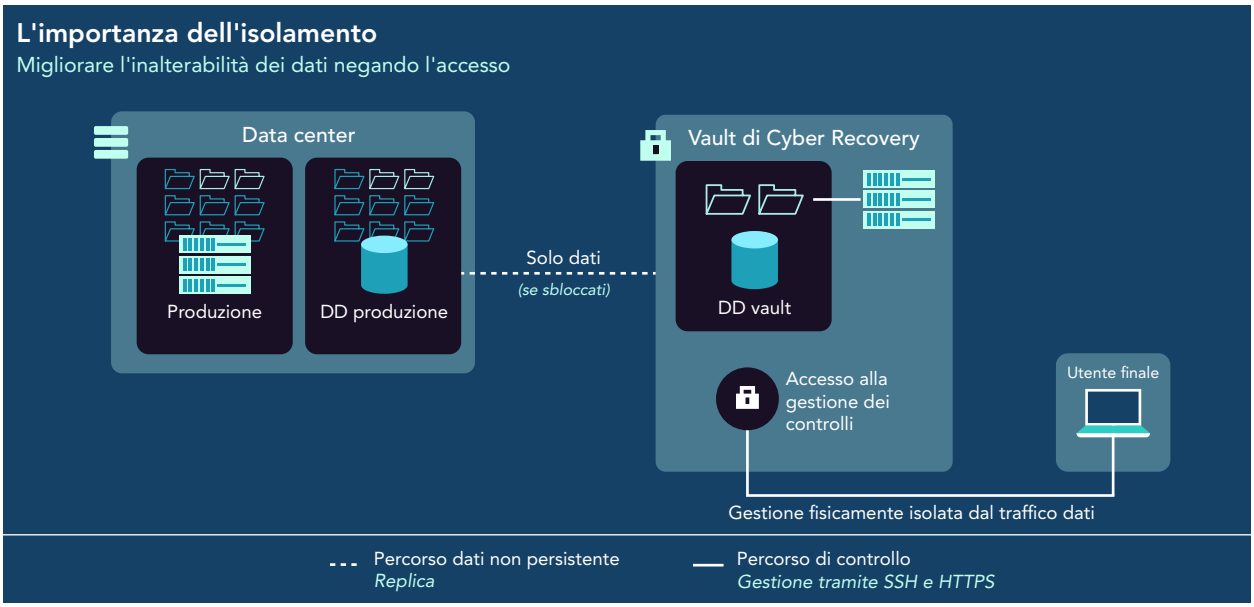

Figura 1. Architettura ad alto livello dei dati e del percorso di controllo del Cyber Recovery Vault. Fonte: Principled Technologies.

Per ulteriori informazioni sui componenti chiave della soluzione Dell PowerProtect Cyber Recovery, consulta Dell PowerProtect Cyber Recovery Solution Guide.

Panoramica di Rubrik Security Cloud

Rubrik descrive Rubrik Security Cloud come una piattaforma Software-as-a-Service (SaaS) che consente ai clienti di "mantenere al sicuro i dati, monitorare i rischi correlati ed eseguirne rapidamente il ripristino, ovunque si trovino, all'interno dell'azienda, nel cloud e nelle applicazioni SaaS".[4] Rubrik afferma di aver sviluppato la soluzione su un'"architettura di microservizi sicura che utilizza servizi ad alta disponibilità e un'infrastruttura in esecuzione su Google Cloud Platform (GCP)"[5]. La Figura 2 mostra la struttura generale di Rubrik Security Cloud.

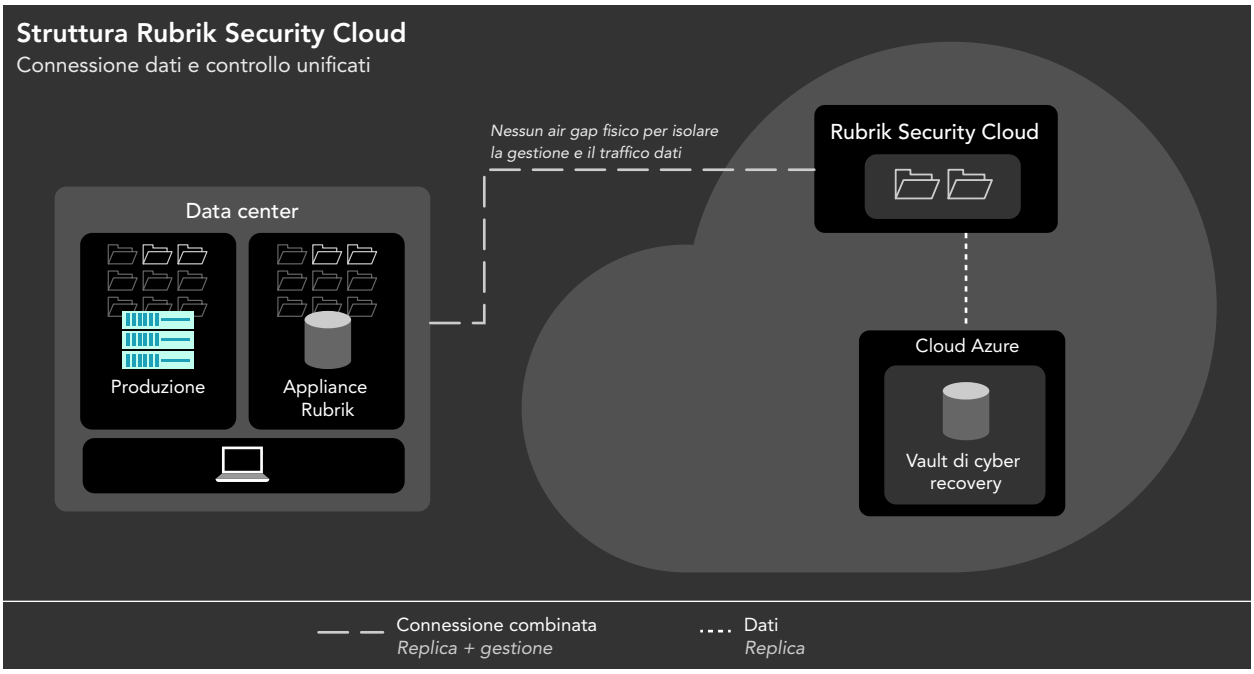

Figura 2. La struttura generale di Rubrik Security Cloud. Fonte: Principled Technologies.

Supporto delle funzioni

Vault di ripristino

I vault sono spazi di storage dedicati che ospitano copie crittografate dei backup che la soluzione esegue all'interno dell'ambiente di produzione. I vault non fanno parte delle soluzioni di backup per la produzione; ciascuno funge invece da posizione isolata di "backup nel backup" da cui i clienti possono ripristinare i backup convalidati.

Dell offre diverse opzioni di vault, tra cui on-premise, presso un sito di colocation remoto o all'interno di un public cloud. Il vault on-premise sfrutta un PPDD operativo air gap che risiede nel proprio data center, potenzialmente anche all'interno dello stesso rack della soluzione di backup. Di norma, una soluzione air gap è isolata fisicamente dall'ambiente di produzione. Un vault in colocation con altri ma off-site, richiede connessioni di rete dedicate a un vault fisico, come ad esempio una versione on-premise, ma il vault è geograficamente separato in un data center remoto. Dell fornisce inoltre vault all'interno del public cloud, collaborando con i provider di servizi cloud Amazon Web Services (AWS), Microsoft Azure e Google Cloud. I vault di public cloud possono offrire flessibilità di configurazione per soddisfare le esigenze dei clienti[6, 7, 8].

Rubrik Cyber Recovery è un componente di Rubrik Security Cloud. Fornito tramite un modello software-as-a-Service, il vault di ripristino utilizza solo lo storage su Microsoft Azure. Molti dei documenti disponibili per il pubblico identificati nel corso della ricerca collegano il vault di Rubrik Cyber Recovery al Rubrik Cloud Vault, il tier di backup, che offre immutabilità[9, 10]. Per questo vault non è necessario altro hardware e può essere utilizzato da qualsiasi versione della piattaforma CDM (Cloud Data Management) Rubrik, a partire dalla 6.02.

Inalterabilità

L'immutabilità si riferisce alla condizione di essere immutabile o permanente. I backup immutabili e le copie di backup consentono agli amministratori di creare permanenze per i file che gli utenti o i sistemi non possono modificare o eliminare fino a quando non è trascorso un intervallo di tempo assegnato. I file vengono quindi "eliminati", cioè rimossi automaticamente dalla soluzione. Le soluzioni eseguono in genere questo processo tramite policy o definizioni che governano il modo in cui il sistema tratta i file.[11]

L'immutabilità di Dell PowerProtect Cyber Recovery si basa sui blocchi di retention, tramite la funzionalità Retention Lock, per impedire l'eliminazione o la modifica (per un periodo di tempo) o la scadenza anticipata forzata delle copie di backup (PPDD è un file system append-only, indipendentemente dal fatto che l'organizzazione abbia abilitato o meno Retention Lock[12]). I clienti Dell gestiscono i backup utilizzando gli MTree PPDD, ovvero partizioni logiche definite dall'utente con impostazioni di retention indipendenti, che assegnano come destinazioni delle applicazioni di backup.[13] I clienti possono scegliere tra due tipi di blocchi di retention: governance e compliance. I blocchi di compliance sono i più rigidi e sicuri dei due. I clienti abilitano i blocchi di retention per MTree, il che significa che tutti i file all'interno di un determinato MTree aderiscono alla definizione di blocco di retention per tale MTree e impostano la durata della retention a livello di file. Una volta definito un blocco di retention di tipo compliance da parte dei clienti, nessun utente o sistema può rimuoverlo. Un amministratore può ripristinare un blocco di retention di tipo governance, l'opzione meno rigida[14].

L'immutabilità della soluzione Rubrik si basa inoltre sui blocchi di retention per impedire la cancellazione o la scadenza anticipata forzata delle copie di backup. Come PowerProtect Cyber Recovery, la soluzione Rubrik aggiunge nuovi dati al file system anziché sovrascrivere quelli esistenti. La soluzione rileva i dati in ingresso e li archivia assieme agli altri. **La soluzione Rubrik non abilita i blocchi di retention per impostazione predefinita** e i clienti devono aprire un ticket diretto al supporto Rubrik o abilitare una regola per due persone per consentire i blocchi di retention. Prima di Rubrik Cloud Data Management versione 7.0.1, i clienti dovevano contattare il supporto Rubrik per abilitare i blocchi di retention; la documentazione di Rubrik non chiarisce se i clienti possono comunque contattare il supporto affinché questa operazione funzioni o meno. Una volta che i clienti hanno abilitato queste funzioni, i blocchi di conservazione impediscono agli utenti o ai sistemi di eliminare i dati al di fuori dei parametri definiti. I blocchi di retention Rubrik richiedono un server NTP (Network Time Protocol) esterno per la sincronizzazione dell'ora, fattore che potrebbe rappresentare un'opportunità per gli utenti malintenzionati di manipolare la sorgente NTP di riferimento e quindi far scadere anticipatamente i blocchi di retention[15].

"La soluzione Rubrik non abilita i blocchi di retention per impostazione predefinita e i clienti devono aprire un ticket diretto al supporto Rubrik o abilitare una regola per due persone per consentire i blocchi di retention."

Licenze e abbonamenti

Dell PowerProtect Cyber Recovery è una soluzione con licenza. In fase di installazione, per impostazione predefinita Dell installa una licenza di valutazione di 90 giorni. Dopo 90 giorni, i clienti devono acquistare una nuova licenza per continuare a utilizzare il prodotto. Dell offre licenze standard (permanenti) e basate su abbonamento.

Rubrik integra Rubrik Cyber Recovery in Rubrik Security Cloud (RSC). I clienti devono disporre di un abbonamento a Rubrik Enterprise Edition per utilizzare Rubrik Cyber Recovery. I termini di abbonamento sono di tre anni.[16, 17] In caso di errore RSC, i carichi di lavoro SAP HANA e Db2 richiedono strumenti di terze parti per ripristinare i dati, il che potrebbe comportare costi di abbonamento aggiuntivi.[18]

Accesso al software di gestione

La gestione del sistema Dell PowerProtect Cyber Recovery avviene in locale, indipendentemente dalla topologia scelta dai clienti per il deployment. Poiché la soluzione avvia il ripristino dal vault, gli amministratori accedono all'interfaccia utente di gestione da qualsiasi luogo in cui sia il vault. Nei casi di attacchi Denial of Service (DoS) o di protezione dei dati, i vault on-premise offrono agli amministratori l'accesso locale senza la

necessità di quello a Internet, che gli attacchi informatici possono gravemente compromettere, interrompendo la connessione a Internet, come raccomandato dal National Institute of Standards and Technology (NIST). I vault in colocation consentono l'accesso fisico all'appliance da un sito remoto e utilizzano connessioni al di fuori della rete Internet pubblica. I vault basati su cloud richiederebbero l'accesso a Internet per il ripristino, elemento che potrebbe ritardare il ripristino on-site fino alla fine dell'attacco informatico e alla ripresa della normale connettività di rete.

Per la gestione di Rubrik Cyber Recovery è necessario accedere a Rubrik Security Cloud, che a sua volta richiede l'accesso a Internet. Come notato, questo tipo di connettività può ritardare il ripristino on-site fino a quando la funzionalità di rete non torna normale in seguito a un attacco informatico.

Poiché i clienti devono avere accesso a RSC per utilizzare le funzionalità di Rubrik Cyber Recovery, RSC diventa un singolo punto di errore. Se quel servizio diventasse inaccessibile, ostacolerebbe il recupero dei dati dall'archivio per il cliente interessato. Rubrik è in grado di ripristinare 10 carichi di lavoro durante un'interruzione del servizio RSC, ma due carichi di lavoro dei database richiedono strumenti di terze parti e l'ausilio del supporto Rubrik per ripristinarli[19, 20]. Inoltre, gli account amministratore compromessi o gli utenti malintenzionati con accesso alla piattaforma RSC avrebbero accesso all'intera proprietà, anziché a un singolo vault.

Ottieni ulteriore assistenza con Managed Detection and Response di Dell

Alcune organizzazioni potrebbero non sentirsi a proprio agio con un approccio "fai da te" alla sicurezza informatica. Dell offre a questi clienti Managed Detection and Response (MDR), un servizio completamente gestito che monitora e rileva minacce e rischi e collabora con i clienti per mitigarli. Secondo Dell, il servizio offre quanto segue:[21]

- Supporto affidabile, tra cui consulenza di esperti per il deployment e la configurazione delle piattaforme di analisi della sicurezza XDR (Extended Detection and Response) supportate da Dell
- Risposta alle minacce e configurazione della sicurezza, con un massimo di 40 ore di configurazione della sicurezza correlata al servizio incluse ogni trimestre
- Rilevamento e analisi 24 ore su 24, 7 giorni su 7, inclusa la ricerca proattiva delle minacce specifica per l'ambiente di ciascun cliente per individuare nuove minacce o varianti di minacce già note in grado di eludere i sistemi di sicurezza
- Avvio della risposta agli incidenti informatici, incluse 40 ore di assistenza remota annuali per la risposta agli incidenti che consentono un avvio rapido delle attività di indagine

Se abbinato ad APEX Cyber Recovery Services, MDR consente ai clienti di scegliere tra molte opzioni per monitorare, rilevare e mitigare minacce e rischi. La disponibilità di opzioni potrebbe significare una copertura estesa o un approccio ibrido che si adatti alle esigenze dell'organizzazione.

Per ulteriori informazioni su MDR, visitare la pagina all'indirizzo **https://www.dell.com/en-us/dt/services/managed-services/managed-workplace-services/managed-detection-response.htm**.

Continuità

Configurazione

La configurazione di Dell PowerProtect Cyber Recovery consiste nell'installazione del software su un sistema Linux o nella creazione di un appliance VMware® vSphere® da un modello Open Virtualization Format (OVF). L'installazione del software prevede 14 passaggi[22], mentre il deployment alternativo dell'appliance vSphere ne prevede 8 per un totale di 5 minuti[23]. Dopo l'installazione, gli amministratori possono accedere alla soluzione tramite web browser dall'interno dell'ambiente isolato.

I clienti devono installare separatamente CyberSense, un motore di analisi della sicurezza intelligente completamente automatizzato e integrato.[24] Le istruzioni per l'installazione di CyberSense in Dell PowerProtect Cyber Recovery non sono disponibili pubblicamente.[25]

Dell dispone di numerose metriche che gli utenti possono ottimizzare, tra cui obiettivo di rilevamento della distruzione (Destruction Detection Objective, DDO), obiettivo di valutazione della distruzione (Destruction Assessment Objective, DAO), punto di Cyber Recovery (Cyber Recovery Point, CRP), tempo di Cyber Recovery (Cyber Recovery Time, CRT), intervallo di sincronizzazione di Cyber Recovery e numero di copie dei dati di Cyber Recovery. Dell consiglia inoltre di caratterizzare i dati che necessitano di protezione. Questi dati possono essere mission-critical, business-critical, dipendenti dai servizi di infrastruttura di base o da altre applicazioni, oppure generali, come ad esempio file binari delle applicazioni, immagini di avvio e cataloghi di backup. La gamma di opzioni offre ai clienti il pieno controllo del proprio ambiente di backup e la possibilità di personalizzare la classificazione dei dati. I servizi di consulenza Dell possono anche fornire ulteriore assistenza e suggerimenti.[26]

Anche la configurazione di Rubrik prevede più passaggi. Prima di creare un cluster, i servizi di supporto Rubrik devono installare e configurare Rubrik CDM. Un amministratore scarica e installa la versione più recente o desiderata di CDM (15 passaggi).[27] Successivamente, l'amministratore può configurare un cluster Rubrik utilizzando l'interfaccia utente o la CLI. È possibile configurare il cluster tramite l'interfaccia utente o la CLI; entrambi gli approcci prevedono 24 passaggi[28, 29]. L'amministratore può quindi registrare i cluster Rubrik adottando un metodo online (12 passaggi)[30] o offline (18 passaggi).[31] Successivamente, l'amministratore abilita l'autenticazione a più fattori (MFA), che richiede 13 passaggi.[32] Infine, l'amministratore aggiunge l'account iniziale (6 passaggi) e qualsiasi altro account.[33] La Figura 3 mostra il numero massimo di passaggi possibili per configurare ciascuna soluzione di ripristino dopo un attacco informatico.

I clienti Rubrik non sono in grado di ottimizzare altre metriche, fattore che potrebbe ridurre la flessibilità necessaria per soddisfare le loro esigenze. Un revisore afferma: "La maggior parte dell'interfaccia utente è piuttosto semplice e intuitiva, ma in alcune aree manca una descrizione della destinazione d'uso dell'opzione oppure l'opzione stessa è assente. Pur semplificando l'esperienza utente, molti dei parametri ottimizzabili non sono presenti ed è necessario aprire un tunnel di supporto affinché un tecnico del supporto possa apportare modifiche all'ambiente del cliente"34.

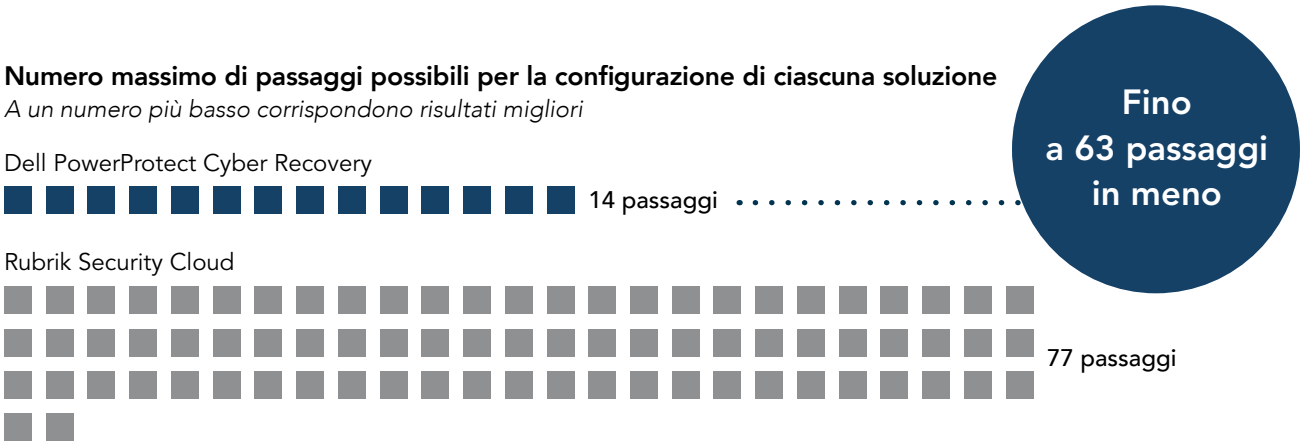

Figura 3. Il numero massimo di passaggi possibili per configurare Dell PowerProtect Cyber Recovery e Rubrik Security Cloud. A un numero più basso corrispondono risultati migliori. Fonte: Principled Technologies.

Manutenzione

Abbiamo osservato che, dopo la configurazione, le interfacce utente di Dell e Rubrik per l'esecuzione delle operazioni quotidiane di manutenzione sono simili. Dopo la configurazione, i clienti possono configurare Dell PowerProtect Cyber Recovery in modo che esegua le seguenti operazioni:[35, 36]

- Generare automaticamente report sui processi di Cyber Recovery in base a una pianificazione e in risposta a una richiesta manuale dell'utente
  - Un utente o una pianificazione crea processi all'avvio di un'operazione di policy, ripristino, backup del sistema o pulizia
- Monitora automaticamente lo stato del vault, la capacità di storage, le operazioni di Cyber Recovery, gli avvisi in caso di errore di copia/sincronizzazione o se il vault di Cyber Recovery è inattivo e i processi di Cyber Recovery
- Esegue automaticamente e in continuo la scansione per individuare gli attacchi e visualizza gli avvisi CyberSense, in ordine di gravità, indicando il numero di file, host, policy interessate, minaccia specifica rilevata, il momento dell'attacco in modo da poter individuare un backup pulito e un elenco di file danneggiati da utilizzare nell'analisi degli attacchi

Analogamente, i clienti possono configurare Rubrik in modo che esegua le seguenti operazioni:[37]

- Utilizzare automaticamente il Rubrik Security Cloud per monitorare, tracciare e visualizzare tutti gli eventi di tutti i cluster Rubrik collegati. Fornisce tre tipi di eventi:[38]
  - Critico - Eventi che richiedono attenzione, come un backup fallito, un archivio o una replica.
  - Avvertenza - Un backup, un archivio o un ripristino sono stati completati
  - Informativo - Solo informazioni
- Esegue automaticamente e in continuo la scansione delle snapshot per individuare indicatori di compromissione nuovi ed esistenti utilizzando Threat Monitor, che fornisce l'ora dell'ultima acquisizione di una snapshot da parte della soluzione, la cronologia degli eventi, l'ora di rilevamento, il numero di file modificati, il numero di file sospetti, il nome del cluster, il tipo e il nome dell'oggetto

Supporto dei carichi di lavoro anomali

Entrambe le soluzioni Rubrik Security Cloud Data Threat Analytics e CyberSense analizzano più tipologie di carichi di lavoro, ma secondo le fonti rilevate, CyberSense supporta carichi di lavoro di rilevamento delle anomalie due volte superiori. Ciò include la scansione dei seguenti tipi di carichi di lavoro:

- Macchine virtuali
- Infrastruttura centrale
- File utente che potrebbero contenere documenti, contratti e proprietà intellettuale
- Database
- Backup effettuati da altri client

"Se contiamo il numero di carichi di lavoro supportati individuati nei dati disponibili al pubblico, scopriamo che CyberSense supporta 21 carichi di lavoro di rilevamento delle anomalie, mentre Rubrik ne supporta 7."

Se contiamo il numero di carichi di lavoro supportati individuati nei dati disponibili al pubblico, scopriamo che CyberSense supporta 21 carichi di lavoro di rilevamento delle anomalie, rispetto ai 7 supportati da Rubrik. Pertanto, secondo i dati disponibili al pubblico condivisi da ciascuna organizzazione, CyberSense supporta carichi di lavoro due volte superiori rispetto a Rubrik Security Cloud Data Threat Analytics. Maggiore è la quantità di dati che una soluzione di ripristino dagli attacchi informatici riesce ad analizzare, maggiori sono le possibilità di individuare malware subdoli o altri danni.

Supporto dei carichi di lavoro delle VM

I carichi di lavoro delle VM si riferiscono alle applicazioni, ai servizi o alle attività che le VM eseguono su un server host fisico o un ambiente cloud. Poiché questi carichi di lavoro possono variare a livello di funzione e in molti altri modi che potrebbero aumentare la loro esposizione a malware, la scansione delle VM è essenziale. Rubrik Security Cloud Data Threat Analytics, che "include servizi di rilevamento delle anomalie, monitoraggio delle minacce, ricerca delle minacce e ripristino dei dati su una risorsa protetta"[39], supporta la scansione dei seguenti carichi di lavoro delle VM[40]:

- VMware
- Nutanix® AHV
- MicroSoft Hyper-V
- Microsoft Azure

CyberSense supporta la scansione dei seguenti carichi di lavoro di VM:[41, 42, 43]

- VMware
- Amazon Web Services (AWS)
- Hyper-V, con backup Dell Avamar o Dell NetWorker

VMware afferma che "fino all'80% dei carichi di lavoro virtualizzati viene eseguito sulla tecnologia VMware."[44] Nel primo trimestre del 2024, Amazon Web Services (AWS), il vendor più diffuso nel mercato dei servizi di infrastruttura cloud, controllava il 31% dell'intero mercato. Microsoft Azure è al secondo posto con una quota di mercato del 25%.[45]

Infrastruttura centrale

L'infrastruttura di base è composta dalle componenti e servizi fondamentali che consentono il funzionamento di un ambiente tecnologico. Individuare malware a questo livello può contribuire a ridurre la gravità di un attacco, perché la funzionalità di infrastruttura di base può influenzare molti sistemi e utenti. La documentazione di Rubrik Security Cloud non menziona il supporto per la scansione di qualsiasi infrastruttura di base.[46]

Al contrario, CyberSense supporta la scansione delle seguenti infrastrutture di base:[47]

- Active Directory
- DNS
- LDAP

File utente che potrebbero contenere documenti, contratti e proprietà intellettuale

Rubrik Security Cloud Data Threat Analytics supporta la scansione dei seguenti file utente[48]:

- Set di file e dataset NAS
- Gruppi di volumi Windows
- Linux e Windows

CyberSense è in grado di eseguire la scansione dei file utente Linux e Windows.[49]

Scansione dei database

CyberSense 7 a confronto con RSC Data Threat Analytics 0

Database

Le applicazioni possono utilizzare diversi tipi di database per molti motivi, pertanto la capacità di rilevare la presenza di malware in vari database potrebbe essere fondamentale per una risposta rapida. Rubrik Security Cloud Data Threat Analytics è in grado di eseguire il backup dei database, ma non è stata identificata documentazione pubblica in cui sia possibile eseguire la scansione di tali backup di database.

CyberSense supporta la scansione dei seguenti database con scansioni a livello di pagina:[50]

- SQL
- Oracle®
- SAP HANA
- Db2
- PostgreSQL
- Epic® Caché
- MariaDB/MySQL

Backup effettuati da altri client

Alcune organizzazioni potrebbero disporre di backup dei dati da più vendor per garantire ridondanza, conformità alle normative o per altri motivi significativi. La documentazione di Rubrik Security Cloud non fa menzione del supporto per la scansione dei backup effettuati da altri client di backup.[51]

Con un vantaggio evidente in questa categoria, CyberSense supporta la scansione dei backup creati dai seguenti client di backup:[52, 53, 54]

- DNAS
- SQL
- NetWorker
- Veritas NetBackup
- Exchange
- Avamar
- Commvault

Tecnologia di scansione

Rubrik Security Cloud include numerosi strumenti per la scansione e per agevolare la scansione in Data Threat Analytics:

- Rubrik Anomaly Detection mostra i file sospetti, le modifiche apportate alle snapshot[55] e i dettagli delle anomalie come gli incidenti anomali affinché i clienti possano studiarli e utilizzarli nelle indagini sulle snapshot.[56] Il software fornisce anche opzioni di ripristino.[57]
- Rubrik VM Encryption Detection rileva gli attacchi ai file del disco virtuale VMware vSphere[58].
- Rubrik Threat Monitoring mostra informazioni sulle minacce e sulle corrispondenze rilevate[59].
- Rubrik Threat Hunt è una scansione avviata dall'utente per individuare gli indicatori di compromissione[60].
- Rubrik Quarantine isola gli oggetti che vengono visualizzati nel corso di una ricerca di minacce[61].

Rubrik RSC dispone inoltre di connettori Rubrik Backup Service per ogni cluster Rubrik.

I clienti Rubrik devono selezionare lo strumento corretto per la propria attività, potrebbero dover avviare le scansioni manualmente o utilizzare più strumenti per portare a termine il lavoro richiesto. Al contrario, Dell offre un'unica opzione di scansione CyberSense, che i clienti potrebbero ritenere più semplice da gestire e amministrare.

La scansione di CyberSense è più approfondita di quella "solo superficiale" di Rubrik RSC Data Threat Analytics. CyberSense esegue scansioni complete dei contenuti dei file e scansioni a livello di pagina dei database e può rilevare la crittografia parziale dei file.[62] Lo strumento utilizza un database di apprendimento automatico (ML) addestrato da Index Engines su migliaia di minacce ai dati e contiene oltre 200 punti di analisi per rilevare il danneggiamento dei dati.[63] A differenza di Rubrik Threat Monitoring e Threat Hunt, CyberSense non si affida ad agenzie esterne di Threat Intelligence per fornire firme malware. Invece, individua nuove minacce.[64] **CyberSense inoltre non si basa su soglie arbitrarie di modifiche accettabili dei file o livelli di entropia tra snapshot che possono dar luogo a falsi negativi**, né addestra il proprio engine di ML a una baseline del comportamento precedente del cliente[65, 66, 67].

> *"CyberSense inoltre non si basa su soglie arbitrarie delle modifiche accettabili dei file o di entropia tra snapshot che possono dar luogo a falsi negativi…."*

Il software di rilevamento delle anomalie Rubrik si basa esclusivamente sui metadati per determinare se una snapshot è danneggiata prima di eseguire qualsiasi analisi del contenuto. Rispetto al ML in corso di CyberSense, il software Rubrik rileva il danneggiamento dopo aver ottenuto le firme. Il rilevamento delle anomalie di Rubrik deve creare un modello comportamentale per definire la normale baseline di un cliente. Questa operazione può richiedere diversi backup. Il modello comportamentale di Rubrik richiede almeno due backup per creare una baseline delle modifiche tipiche apportate a un file system in assenza di attacchi. Tuttavia, un unico set di statistiche sulle modifiche potrebbe non essere

sufficiente per stabilire ciò che è tipico. Gli eventi aziendali potrebbero innescare più o meno attività o tipologie di attività sospette che non si sono verificate tra la prima e la seconda snapshot di Rubrik. Maggiore è il numero di backup analizzati dalla soluzione Rubrik, maggiore è la precisione con cui è in grado di addestrare il modello comportamentale a una baseline[68, 69].

CyberSense contiene tutte le analisi nel vault. Nella pipeline di analisi del comportamento del file system, Rubrik invia metadati sulle modifiche del file system del cliente alla piattaforma Polaris basata su cloud per eseguire l'analisi del comportamento, aprendo una superficie di attacco[70].

I clienti possono utilizzare Rubrik Threat Monitoring e Threat Hunt solo come parte dell'edizione Rubrik Enterprise.[71] I clienti devono eseguire scansioni di Threat Hunt con privilegi di controllo degli accessi basato sui ruoli (RBAC, Role-Based Access Control) e gli utenti devono indicare quali indicatori specifici di compromissione (IOC) desiderano ricercare.[72] Questa non è la migliore prassi del settore.[73] Come CyberSense, Threat Hunt supporta VMware, AHV, Hyper-V, set di file NAS e server Linux e Windows[74].

Le sezioni seguenti offrono ulteriori dettagli sul modo in cui la soluzione Rubrik offre il rilevamento delle minacce.

Dati di metadati e statistiche del sistema di file.

Il modello comportamentale ML di Rubrik Anomaly Detection registra le modifiche apportate al file system dall'ultima snapshot, ad esempio il numero di file aggiunti, eliminati o spostati, come metadati.[75] Quindi, un modello ML si addestra su queste modifiche per creare una "baseline" del modello comportamentale per il file system. Rubrik contrassegna una snapshot come anomala se rileva un numero eccessivo di modifiche. Dopo che l'analisi del comportamento ha contrassegnato una snapshot, la soluzione avvia un'analisi del contenuto del file[76]. Il monitoraggio dei metadati può aggiungere un livello di sicurezza, ma potrebbe non offrire la protezione necessaria per prevenire o ridurre i tempi di inattività dovuti a un evento.

> *"CyberSense non ha bisogno di una baseline; monitora e analizza le modifiche al contenuto di file e database dalle prime copie di backup."*

Al contrario, **CyberSense non ha bisogno di una baseline; monitora e analizza le modifiche ai contenuti di file e database dalle prime copie di backup.** L'approccio CyberSense offre una maggiore granularità, poiché il software analizza anche parti di un file o singole pagine di un database. Analogamente alla soluzione Rubrik, le scansioni CyberSense includono proprietà dei metadati e i risultati di feed nell'engine di apprendimento automatico (ML). A differenza della soluzione Rubrik, CyberSense non si limita alla scansione dei metadati e Index Engines ha addestrato il proprio engine di ML sugli attacchi documentati da Index Engines, non sulle firme o sui comportamenti precedenti dei clienti[77, 78].

Soglie

Durante l'analisi del comportamento, ML Rubrik determina la probabilità che si sia verificata un'anomalia su un file system. Se la soluzione Rubrik lo ritiene probabile, esegue un'analisi del contenuto. Si potrebbe trattare di una soglia comportamentale modellata, che determina il "comportamento anomalo". Ad esempio, la soluzione Rubrik potrebbe segnalare comportamenti anomali quando rileva molti file nuovi o modificati oppure un aumento degli indicatori di casualità o di crittografia.[79] Durante l'analisi del contenuto, Rubrik Anomaly Detection visualizza le modifiche nel contenuto del file e calcola la probabilità di crittografia quantificando l'entropia del file system. L'entropia di un file system è utile a mostrare la probabilità con cui un attacco ransomware abbia crittografato i file. Se l'entropia supera una soglia di anomalia, la soluzione avvisa l'utente[80, 81]. L'efficacia nel rilevamento del danneggiamento dei dati dipende dal rigore della soglia. Una tolleranza eccessiva potrebbe causare falsi negativi e quindi un falso senso di sicurezza[82]. I clienti devono impostare le soglie in modo appropriato.

Al contrario, CyberSense verifica la crittografia parziale di un file analizzandone il contenuto per garantire un livello di affidabilità del 99,99% (secondo Dell e Index Engines) nel rilevamento del danneggiamento dei dati[83].

Firme ed estensioni dei file

Rubrik Threat Monitoring and Threat Hunt analizzano le snapshot alla ricerca di IOC. Quando una delle molteplici fonti di threat intelligence monitorate da Rubrik rileva un nuovo IOC, Threat Monitoring invia il feed delle minacce contenente le regole YARA (Yet Another Ridiculous Acronym) per l'identificazione del nuovo malware, altrimenti noto come firma malware, a tutti i cluster Rubrik. I cluster iniziano quindi la scansione.[84] Un recente report di WatchGuard suggerisce che il 57,8% dei malware evita il rilevamento delle firme. Attacchi malware avanzati, come ad esempio BianLian, possono impiegare metodi per eludere il riconoscimento delle firme e le nuove varianti di malware possono presentare firme leggermente diverse rispetto all'originale. Di conseguenza, potrebbe essere più difficile per la threat intelligence rimanere aggiornata[85].

In confronto, CyberSense utilizza oltre 200 analisi e fornisce un modello di apprendimento automatico addestrato su migliaia di varianti di ransomware. Index Engines ha dimostrato che il metodo CyberSense è in grado di rilevare varianti sofisticate e mai viste prima senza dover scaricare firme[86], il che rappresenta un ulteriore vantaggio nel non dover dipendere da Internet nel corso di un evento.

Eventi di crittografia di massa

La soluzione Rubrik monitora gli eventi di crittografia di massa elaborando l'entropia dell'intero file system.[87] CyberSense è molto più granulare. Non solo esegue la scansione del file system in generale o anche di ogni singolo file, ma esegue la scansione di parti del contenuto interno dei file. Secondo Index Engines, il calcolo dell'entropia esclusivamente su un singolo file anziché su sue singole parti "rileva solo la crittografia estrema dell'intero file" o gli eventi di crittografia di massa[88].

Ripristinabilità

Sulla base della documentazione, consideriamo il ripristino con Dell PowerProtect Cyber Recovery un processo più semplice e snello rispetto al ripristino con Rubrik. Questa sezione del report, incluse le relative sottosezioni, confronta le funzionalità di ripristino delle due soluzioni e il modo in cui queste ultime le implementano.

La documentazione di Rubrik indica quali delle funzioni di ripristino funzionano per i tipi di VM. Questo può sembrare un utile livello di granularità, ma le numerose clausole e varianti rendono complesso il ripristino. Ad esempio, quando i clienti Rubrik devono ripristinare dati, file e sistemi, devono selezionare gli oggetti snapshot che desiderano includere nel piano di ripristino. Dopo aver creato uno o più piani di ripristino, Rubrik offre numerose opzioni in tal senso, tra cui[89, 90, 91, 92, 93]:

- ripristino dei file tramite download o sovrascrittura e ripristino in una cartella separata, esportazione in un host diverso o esportazione in un servizio in cluster
- ripristino dei file per le VM tramite download o sovrascrittura e ripristino in una cartella separata o esportazione in un'altra macchina virtuale
- ripristino completo delle snapshot di una VM o di una snapshot del disco come segue:
  - Live Mount, che crea una nuova VM dalla snapshot.
  - Montaggio di dischi virtuali, che crea nuovi dischi virtuali dalla snapshot.
  - Ripristino istantaneo, che sostituisce la VM corrente con una nuova VM creata dalla snapshot.
  - Esportazione, che crea una nuova VM a partire dallo snapshot in un datastore selezionato.
  - Ripristino in batch delle VM
- Cyber Recovery in blocco per piani di ripristino tramite Live Mount ed esportazione.
- Ripristino di Rubrik Security Cloud Orchestrated Application per il ripristino di emergenza della VM in un sandbox isolato, un sito remoto o in loco.

Il ripristino batch di Rubrik dimostra ulteriormente la complessità. Nella tabella 1 sono presentate le funzionalità di ripristino batch fornite da Rubrik a seconda dell'hypervisor.[94]

Tabella 1: Le funzionalità di ripristino batch fornite da Rubrik sono adatte a diversi hypervisor. Fonte: Rubrik.

Opzioni di creazione delle VM				
	Live Mount	**Live Mount con migrazione opzionale**	**Export**	**Ripristino istantaneo**
Macchine virtuali vSphere	Disponibile, utilizza il cluster Rubrik come datastore	Non disponibile	Disponibile, utilizza il datastore del hypervisor recuperato	Disponibile, utilizza il cluster Rubrik come datastore
Macchine virtuali AHV	Disponibile, utilizza il cluster Rubrik come datastore	Disponibile, utilizza il cluster Rubrik come datastore e il container Nutanix per tutte le scritture successive	Disponibile, utilizza il container Nutanix come datastore	Non disponibile
Macchine virtuali Hyper-V	Disponibile, utilizza il cluster Rubrik come datastore	Non disponibile	Disponibile, utilizza il datastore del hypervisor recuperato	Disponibile, sostituisce la VM corrente con una nuova dalla snapshot Utilizza il cluster Rubrik come datastore.

Per la soluzione Rubrik, l'archivio dati ripristinato si trova in genere nel cluster Rubrik e non nell'ambiente di produzione, il che può creare problemi. Questi problemi vengono presentati nella sezione successiva, "Limitazioni di Rubrik". Al contrario, PowerProtect è in grado di collocare i dati ripristinati in ambienti di ripristino o di produzione per contribuire a garantire un ripristino più rapido e fluido, riducendo al minimo i tempi di inattività.

La tabella 2 mostra ulteriori informazioni fornite da Rubrik sul ripristino delle VM vSphere.[95] Come mostrato nella tabella, la maggior parte dei datastore di ripristino vSphere si trova nel cluster Rubrik.

Tabella 2: Funzionalità di ripristino fornite da Rubrik per le VM vSphere. Fonte: Rubrik.

Funzionalità di ripristino fornite da Rubrik per vSphere				
Action	**Datastore**	**Stato di alimentazione**	**Network**	**Source VM**
Ripristino dei file	Non applicabile	Non applicabile	Non applicabile	Nessun impatto
Live Mount	Cluster Rubrik locale	Acceso o spento	Disconnesso	Nessun impatto
Mount dischi virtuali	Cluster Rubrik locale	Attivo	Disconnesso	Nessun impatto
Ripristino istantaneo	Cluster Rubrik locale	Attivo	Connessa (opzionale)	Spenta e rinominata
Export	Datastore dell'hypervisor	Spento	Disconnesso	Nessun impatto
Recupero in situ	Datastore dell'hypervisor	Attivo	Uguale alla VM di origine	Il ripristino in loco sovrascrive i file del disco virtuale della VM di origine con i dati del disco virtuale dalla snapshot, senza modificare le proprietà della VM

La soluzione Rubrik non implementa ampiamente il ripristino di massa e le opzioni di ripristino di massa sono limitate e complesse. Come spiegato più avanti nella sezione "Dell PowerProtect Data Manager offre l'equivalente del "ripristino di massa" di Rubrik" del presente report, Dell PowerProtect è una soluzione più snella e semplice.

Sfatare il mito del ripristino di massa

Rubrik pubblicizza il ripristino di massa, che definisce come il ripristino rapido delle operazioni aziendali tramite il ripristino di app, file o utenti su larga scala.[96] Offrono molte opzioni di ripristino in blocco. Tuttavia, la soluzione Rubrik in genere archivia i dati ripristinati nel cluster Rubrik e non nell'ambiente di produzione.[97] I carichi di lavoro dipendono dalla disponibilità del sistema Rubrik fino al completamento della migrazione della soluzione. Il cluster Rubrik locale è lo storage tier 3, pertanto i clienti dovrebbero eseguire un'ulteriore migrazione nel proprio ambiente di produzione per tornare ai livelli di prestazioni pianificati. Con questo singolo punto di errore e prestazioni ridotte mentre il sistema completa la migrazione, non possiamo considerare completato il ripristino finché la soluzione Rubrik non ripristina i carichi di lavoro nell'ambiente di produzione.

Dell PowerProtect offre anche il ripristino in blocco consentendo agli utenti di selezionare più VM per il ripristino nell'interfaccia utente di ripristino.

Dell PowerProtect Data Manager offre l'equivalente del "ripristino di massa" di Rubrik

Rispetto alla soluzione Rubrik, anche quella Dell offre diverse opzioni di ripristino equivalenti per le VM vSphere. Dell PowerProtect può collocare i dati delle VM negli ambienti di ripristino o produzione. La maggior parte delle opzioni Rubrik inseriscono i dati solo nel cluster Rubrik. La tabella 3 mostra le opzioni di ripristino Dell.[98, 99, 100, 101]

Tabella 3: Opzioni di ripristino Dell. Fonte: Principled Technologies.

Opzioni di ripristino Dell	
Type	**Informazioni sulla funzione**
Restore a livello di file	Ripristina solo i file infetti in loco o tramite rollback
VM live	Ripristina una VM nel cluster con la migrazione successiva alla produzione
Ripristina su nuova posizione	Ripristina l'ambiente originale o uno nuovo (ad esempio, una camera bianca o un'infrastruttura di ripristino) e durante il processo gli utenti possono selezionare più VM contemporaneamente per un ripristino in blocco o su vasta scala
Accesso/VM live	Crea una copia isolata dei dati di produzione
Orchestration del ripristino	Consente agli amministratori di pianificare il ripristino o renderlo disponibile su richiesta; priorizza il ripristino automatico delle macchine virtuali in produzione o nell'ambiente di ripristino.

Limitazioni di Rubrik

La soluzione Rubrik mette in quarantena le snapshot infettate da malware per analisi future. Tuttavia, la soluzione Rubrik non mette in quarantena le snapshot per impostazione predefinita. I clienti possono quindi scaricare ed eseguire analisi forensi sui file in quarantena manualmente o per mezzo di strumenti di terze parti, esponendosi potenzialmente al malware[102, 103].

> *CyberSense effettua l'analisi senza richiedere all'utente di eseguire la propria analisi forense e il software automatizza la creazione di punti di ripristino.*

CyberSense analizza file e database per impostazione predefinita. Gli utenti non devono mettere in quarantena le snapshot manualmente. **CyberSense effettua l'analisi senza richiedere all'utente di eseguire la propria analisi forense e il software automatizza la creazione di punti di ripristino.**[104]

Rubrik RSC in modalità di gestione solo RSC rappresenta un singolo punto di errore per numerose funzionalità. Aspetto ancor più preoccupante è che un attacco potrebbe causare un'interruzione del servizio RSC, con conseguenze sulla connettività Internet o sulla connettività tra il sito degli utenti e RSC. Dopo tali attacchi, la soluzione offre agli utenti un insieme limitato di funzionalità, disponibili tramite l'interfaccia utente di Rubrik CDM o l'automazione basata su API, ma solo se gli utenti hanno creato un account di servizio RSC prima dell'attacco[105, 106]. Un'organizzazione può ripristinare i seguenti carichi di lavoro e dati senza RSC: MongoDB, Microsoft Exchange, file, snapshot Hyper-V, Live Mount da volumi gestiti, file host NAS, Oracle, SQL Server, VCD e VMware.[107] Per ripristinare SAP HANA senza RSC sono necessari strumenti di terze parti, come Studio e Cockpit Cross, nonché il supporto Rubrik tramite il tunnel di supporto. Anche per il ripristino di IBM Db2 senza RSC sono necessari strumenti di terze parti IBM e il supporto Rubrik tramite il tunnel di supporto[108].

Air gap/isolamento

Il NIST definisce un air gap come "un'interfaccia tra due sistemi in cui (a) non sono connessi fisicamente e (b) nessuna connessione logica è automatizzata (vale a dire, i dati vengono trasferiti tramite l'interfaccia solo manualmente, sotto controllo umano)."[109]

Gli air gap possono contribuire al controllo del flusso di dati da una sorgente a una destinazione e possono rappresentare un componente importante di qualsiasi strategia di protezione ransomware e di ripristino dagli attacchi informatici. Se un attacco o un evento compromette i sistemi di backup di produzione, la possibilità di impedire il traffico dai sistemi di produzione ai backup protetti nei vault di ripristino dagli attacchi informatici potrebbe rappresentare una soluzione FailSafe.

Isolamento fisico

Nel film "Mission Impossible" si può osservare un esempio di soluzione fisicamente isolata, in cui il personaggio principale ha aggirato tutte le altre misure di sicurezza della struttura per poter accedere a dati sensibili su un sistema informatico non connesso ad alcuna rete esterna. L'isolamento fisico può inoltre utilizzare segmenti di rete fisica dedicata normalmente disconnessi per trasportare le copie di backup dai sistemi di produzione al vault. Quando sono disconnessi, questi air gap operativi creano una barriera fisica che i dati non possono attraversare automaticamente, rendendo l'accesso più difficile per gli utenti malintenzionati.

Le organizzazioni possono isolare fisicamente Dell PowerProtect Cyber Recovery per favorire una strategia di air gap operativi. La soluzione utilizza una connessione fisica dedicata ed esegue la replica dei dati come operazione "pull" dal vault anziché come operazione "push" dalla soluzione di backup. Durante la copia/replica, la soluzione attiva la connessione, crittografa i dati ed esegue la migrazione attraverso la linea dedicata.[110] Dopo aver completato la replica, la soluzione disabilita nuovamente la connessione dal lato del vault. La soluzione rende le copie di archivio immutabili con politiche di conservazione bloccate, in modo che anche se un utente o un sistema ottiene l'accesso, non possono modificare o

eliminare le copie di archivio. Nessun traffico di gestione attraversa il percorso di replica, quindi **anche se gli utenti malintenzionati acquisiscono il controllo della soluzione di backup on-premise, il vault avvia e disconnette il percorso di replica e utilizza estrazioni unidirezionali di soli dati dall'origine dati, limitando così l'accesso diretto al vault**[111].

Isolamento logico

L'isolamento logico, d'altro canto, utilizza sistemi che possono risiedere sulla stessa rete fisica, ma creano una separazione e un controllo di rete logici per garantire che i sistemi non possano inviare dati tra loro. La soluzione utilizza implementazioni di sicurezza aggiuntive, come ad esempio crittografia e hashing insieme a RBAC e autenticazione a più fattori, per garantire che un sistema o un utente non autorizzato non possa leggere i dati che risiedono all'interno di un altro sistema.

Rubrik descrive la sua funzionalità di ripristino dagli attacchi informatici come l'utilizzo di una strategia logica di air gap[112, 113]. Molte delle dichiarazioni pubbliche di Rubrik disponibili mettono in dubbio la necessità di air gap. Una presentazione di Rubrik intitolata "Rubrik Security – Air Gap and Immutability" sostiene che la soluzione nativa proposta è air gapped perché non c'è modo di accedere o modificare i backup una volta che li esegue, anche se l'appliance Rubrik rimane sulla rete fisica.[114] Tuttavia, un utente malintenzionato autenticato potrebbe comunque accedere all'interfaccia utente grafica dell'appliance, con conseguenti ripercussioni sul ripristino. Per attenuare questo problema, Rubrik dispone di blocchi di retention che impediscono la scadenza dei backup, rendendoli immutabili. Una volta abilitato, il blocco della conservazione impedisce anche al cluster Rubrik di essere ripristinato alle impostazioni di fabbrica e cancellato. Secondo la Rubrik CDM Security Guide, la soluzione disattiva globalmente i blocchi di retention sul cluster per impostazione predefinita e richiede ai clienti di contattare il supporto Rubrik per abilitarli[115]. Le fonti disponibili al pubblico non chiariscono se il supporto Rubrik sia in grado di disabilitare anche i blocchi di retention. Tale condizione solleva il timore che un malintenzionato autorizzato sia comunque in grado di aggirare i livelli di sicurezza.

"Nessun traffico di gestione attraversa il percorso di replica, quindi anche se gli utenti malintenzionati acquisiscono il controllo della soluzione di backup on-premise, il vault avvia e disconnette il percorso di replica e utilizza estrazioni unidirezionali di soli dati dall'origine dati, limitando così l'accesso diretto al vault."

Conclusioni

Le organizzazioni devono prendere in considerazione attivamente numerosi vettori di attacco nei propri data center. Un buon piano di protezione dei dati cerca di proteggere tutti i dati, in particolare i dati critici essenziali per le operazioni. Abbiamo esaminato le informazioni pubblicamente disponibili per Dell PowerProtect Cyber Recovery e Rubrik Secure Cloud per scoprire in che modo entrambe le soluzioni affrontano la gestione, la protezione e il ripristino dei dati.

PowerProtect Cyber Recovery isola fisicamente le copie di backup dei dati critici in un vault e ne garantisce il ripristino in caso di attacco informatico. La soluzione impiega una strategia di air gap operativi con isolamento fisico, un aspetto che Rubrik Secure Cloud non può affermare e si basa sull'isolamento logico.

Cyber Recovery utilizza l'analisi basata su ML in CyberSense per valutare l'integrità dei dati nel vault e identificare i dati di backup puliti per il ripristino. Rubrik Secure Cloud, al contrario, offre uno strumento di analisi addestrato all'apprendimento automatico che cerca anomalie anziché eseguire scansioni approfondite sui file.

Inoltre, la soluzione Cyber Recovery offre molteplici opzioni di ripristino, sfruttando i dati non compromessi provenienti dal vault per favorire un ritorno efficiente e rapido alle operazioni. In molti casi, PowerProtect Cyber Recovery può offrire funzionalità e vantaggi di cui Rubrik Secure Cloud non dispone, offrendo così una soluzione potenzialmente più sicura e in grado di eseguire analisi più approfondite per ridurre al minimo i tempi di inattività e accelerare il ripristino.

---

1. Anastasia Dergacheva and Jesse R. Taylor, "Study Finds Average Cost of Data Breaches Continued to Rise in 2023," consultato il 25 luglio 2024, https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/03/study-finds-average-cost-of-data-breaches-continued-to-rise-in-2023.
2. Dell, "Dell PowerProtect Cyber Recovery Solution Guide," consultato il 18 aprile 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
3. Dell, "Dell PowerProtect Cyber Recovery Solution Guide."
4. Rubrik, "Rubrik Security Cloud Architecture and Security Implementation," consultato il 18 aprile 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.
5. Rubrik, "Rubrik Security Cloud Architecture and Security Implementation," consultato il 18 aprile 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.
6. Rob Emsley, "Public Cloud Vault to Secure, Isolate and Recover Data," consultato il 20 marzo 2024, https://www.dell.com/en-us/blog/public-cloud-vault-to-secure-isolate-and-recover-data/.

7. Brian White, "Dell's PowerProtect Cyber Recovery Expands to Microsoft Azure," consultato il 20 marzo 2024, https://www.dell.com/en-us/blog/dells-powerprotect-cyber-recovery-expands-to-microsoft-azure/.
8. Dell, "Cyber Recovery on Google Cloud Platform," consultato il 20 marzo 2024, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-cyber-recovery-reference-architecture/cyber-recovery-on-google-cloud-platform/.
9. Chris Mellor, "Up to $5m compensation if Rubrik Cloud Vault recovery busted," consultato il 20 marzo 2024, https://blocksandfiles.com/2022/02/24/up-to-5m-compensation-if-rubrik-cloud-vault-recovery-busted/.
10. Kristina Avrionova, "Frequently Asked Questions about Rubrik Cloud Vault," consultato il 20 marzo 2024, https://www.rubrik.com/blog/company/22/3/faq-about-rubrik-cloud-vault.
11. Chris Wahl, "Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture," consultato il 22 marzo 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
12. Dell, "Data Domain Invulnerability Architecture: Enhancing Data Integrity and Recoverability," consultato il 7 giugno 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h7219-data-domain-data-invul-arch-wp.pdf.
13. Dell, "Consolidate Governance and Compliance Archive Data," consultato il 4 aprile 2024, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-domain-retention-lock/consolidate-governance-and-compliance-archive-data/.
14. Dell, "Dell PowerProtect Cyber Recovery Solution Guide," consultato il 24 marzo 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
15. Rubrik, "Retention-locked SLA Domain attributes," consultato il 2 aprile 2024, https://docs.rubrik.com/en-us/8.0/ug/cdm/attributes_of_retention_locked_sla_domains.html.
16. Rubrik, "Rubrik Cyber Recovery," consultato il 20 marzo 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/brf-rubrik-cyber-recovery.pdf.
17. Rubrik, "Rubrik Licensing: Subscribe to Simplicity," consultato il 20 marzo 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/data-sheet/rubrik-licensing-data-sheet.pdf.
18. Rubrik, "Workloads require third-party tools for recovery," consultato il 6 maggio 2024, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.
19. Rubrik, "Recoverable workloads during RSC service disruption," consultato il 6 maggio 2024, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.
20. Rubrik, "Workloads require third-party tools for recovery."
21. Dell, "Strengthen your security posture with Managed Detection and Response," consultato il 2 aprile 2024, https://www.delltechnologies.com/asset/pl-pl/services/managed-services/technical-support/managed-detection-and-response-datasheet.pdf.
22. Dell, "Dell PowerProtect Cyber Recovery 19.13 Installation Guide," consultato il 20 marzo 2024, https://www.dell.com/support/manuals/en-us/cyber-recovery/irs_p_19.13_installation/installing-the-cyber-recovery-software?guid=guid-8718978d-ddd0-4dc0-bca7-fb04a2f3d1fb&lang=en-us.
23. Dell, "Dell PowerProtect Cyber Recovery 19.13 Installation Guide."
24. Dell, "Dell PowerProtect Cyber Recovery 19.13 Installation Guide."
25. Dell, "Installing CyberSense in Dell PowerProtect Cyber Recovery," consultato il 20 marzo 2024, https://infohub.delltechnologies.com/en-US/l/ransomware-protection-secure-your-data-on-dell-powerflex-with-powerprotect-cyber-recovery-1/installing-cybersense-in-dell-powerprotect-cyber-recovery-1/.
26. Dell, "Dell PowerProtect Cyber Recovery Solution Guide."
27. Rubrik, "Downloading and installing Rubrik CDM," consultato il 20 marzo 2024, https://docs.rubrik.com/en-us/saas/install/download_install_cdm_on_appliance_nodes.html.
28. Rubrik, "Setting up a Rubrik cluster using the UI," consultato il 20 marzo 2024, https://docs.rubrik.com/en-us/saas/install/setting_up_ui.html.
29. Rubrik, "Setting up a Rubrik cluster using the CLI," consultato il 20 marzo 2024, https://docs.rubrik.com/en-us/saas/install/setting_up_cli.html.
30. Rubrik, "Registering Rubrik clusters using the online method," consultato il 20 marzo 2024, https://docs.rubrik.com/en-us/saas/install/registering_clusters_online.html.
31. Rubrik, "Registering Rubrik clusters using the offline method," consultato il 2 aprile 2024, https://docs.rubrik.com/en-us/saas/install/registering_clusters_offline.html.
32. Rubrik, "Enabling MFA," consultato il 21 marzo 2024, https://docs.rubrik.com/en-us/saas/install/rsc_enabling_mfa.html.
33. Rubrik, "Adding the initial account," 21 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/adding_the_initial_account.html.
34. TrustRadius, "Learning Rubrik by putting the pieces together Brik by Brik," consultato il 21 marzo 2024, https://www.trustradius.com/reviews/rubrik-2023-09-20-21-03-04.
35. Dell, "Dell PowerProtect Cyber Recovery Solution Guide."

36. Index Engines, "CyberSense®: How it Works," consultato il 21 marzo 2024, https://www.indexengines.com/how-it-works.
37. Rubrik, "Anomaly event details," consultato il 21 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_event_details.html.
38. Rubrik, "Events page," consultato il 21 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/common/events_page.html.
39. Rubrik, "RSC Data Threat Analytics," consultato il 21 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/ri_ransomware_monitoring.html.
40. Rubrik, "RSC Data Threat Analytics."
41. Dell Technologies, "Dell PowerProtect Cyber Recovery: Reference Architecture," consultato il 6 maggio 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h18661-dell-powerprotect-cyber-recovery-reference-architecture-wp.pdf.
42. Dell Technologies, "Dell EMC Avamar for Hyper-V," consultato il 16 maggio 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu89876.pdf.
43. Dell Technologies, "Dell EMC NetWorker Module for Microsoft for Hyper-V," consultato il 16 maggio 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu92011.pdf.
44. VMware, "Accelerate IT. Innovate with your cloud.," 9 maggio 2024, https://www.vmware.com/files/pdf/VMware-Corporate-Brochure-BR-EN.pdf.
45. Statista, "Cloud infrastructure services vendor market share worldwide from fourth quarter 2017 to first quarter 2024," 17 luglio 2024, https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/.
46. Rubrik, "RSC Data Threat Analytics."
47. Dell Technologies, "CyberSense® for PowerProtect Cyber Recovery," consultato il 27 giugno 2024, https://www.delltechnologies.com/asset/en-gb/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
48. Rubrik, "RSC Data Threat Analytics."
49. Index Engines, "CyberSense® Support Matrix," consultato il 21 marzo 2024, https://www.indexengines.com/csmatrix.
50. Dell Technologies, "CyberSense® for PowerProtect Cyber Recovery."
51. Rubrik, "Keep Your Databases Running in the Face of Any Threat."
52. Index Engines, "CyberSense® Support Matrix."
53. Dell Technologies, "Dell EMC Avamar for Hyper-V."
54. Dell Technologies, "Dell EMC NetWorker Module for Microsoft for Hyper-V."
55. Rubrik, "Anomaly incidents," consultato il 2 aprile 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_incident.html.
56. Rubrik, "Data Threat Analytics events," consultato il 2 aprile 2024, https://docs.rubrik.com/en-us/saas/saas/ri_events.html.
57. Rubrik, "Viewing Anomaly Detection," consultato il 2 aprile 2024, https://docs.rubrik.com/en-us/saas/saas/viewing_ri_investigations.html.
58. Rubrik, "VM Encryption Detection," consultato il 2 aprile 2024, https://docs.rubrik.com/en-us/saas/saas/vm_encryption_detection.html.
59. Rubrik, "Viewing the Threat Monitoring page," 2 aprile 2024, https://docs.rubrik.com/en-us/saas/saas/viewing_the_threat_monitoring_page.html.
60. Rubrik, "Initiating a threat hunt," consultato il 2 aprile 2024, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
61. Rubrik, "Quarantining matched files or objects," consultato il 2 aprile 2024, https://docs.rubrik.com/en-us/saas/saas/quarantining_matched_objects_or_files.html.
62. Dell, "CyberSense® for PowerProtect Cyber Recovery."
63. Dell, "CyberSense® for PowerProtect Cyber Recovery."
64. Index Engines, "The Power of CyberSense's Machine Learning," consultato il 2 aprile 2024, https://go.indexengines.com/csmachinelearning.
65. Index Engines, "The Power of CyberSense's Machine Learning."
66. Index Engines, "The Power of CyberSense's Machine Learning."
67. Dell, "CyberSense® for PowerProtect Cyber Recovery."
68. Rubrik, "Anomaly Detection behavioral model," consultato il 20 maggio 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_detection_behavioral_model.html.
69. Amazon, "Training ML Models," consultato il 2 aprile 2024, https://docs.aws.amazon.com/machine-learning/latest/dg/training-ml-models.html.
70. Rubrik, "Defense in Depth with Polaris Radar," consultato il 21 marzo 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/Defense-In-Depth-Polaris-Radar-Technical-White-Paper.pdf.
71. Rubrik, "Data Threat Analytics dashboard," consultato il 21 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/ri_dashboard.html.
72. Rubrik, "Initiating a threat hunt," consultato il 21 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
73. SentinelOne, "What Is A Malware File Signature (And How Does It Work)?" consultato il 4 aprile 2024, https://www.sentinelone.com/blog/what-is-a-malware-file-signature-and-how-does-it-work/.

74. Rubrik, "Threat hunts," consultato il 21 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/ri_threat_hunts.html.
75. Rubrik, "Anomaly Detection features," consultato il 22 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
76. Rubrik, "Behavioral model."
77. Index Engines, "The Power of CyberSense's Machine Learning."
78. Dell, "CyberSense® for PowerProtect Cyber Recovery."
79. Rubrik, "Behavioral model."
80. Rubrik, "Anomaly Detection features."
81. Rubrik, "Behavioral model."
82. Dell, "CyberSense® for PowerProtect Cyber Recovery."
83. Morningstar, "Index Engines' CyberSense Announces 99.99% SLA in Detecting Ransomware Corruption, Empowering Smarter Recovery," consultato il 17 luglio 2024, https://www.morningstar.com/news/pr-newswire/20240618ny41171/index-engines-cybersense-announces-9999-sla-in-detecting-ransomware-corruption-empowering-smarter-recovery.
84. Rubrik, "Threat Monitoring," consultato il 22 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/threat_monitoring.html.
85. Index Engines, "The Power of CyberSense's Machine Learning."
86. Index Engines, "The Power of CyberSense's Machine Learning."
87. Rubrik, "Anomaly Detection features," consultato il 22 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
88. Index Engines, "The Power of CyberSense's Machine Learning."
89. Rubrik, "Investigating and recovering anomalous files for filesets," consultato il 22 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files.html.
90. Rubrik, "Investigating and recovering anomalous files for virtual machines," consultato il 22 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files_for_virtual_machines.html.
91. Rubrik, "Full snapshot recovery of a virtual machine," consultato il 22 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/full_snapshot_recovery_of_a_virtual_machine.html.
92. Rubrik, "Recovery of a batch of virtual machines," consultato il 22 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
93. Rubrik, "Performing bulk recovery for Recovery Plans," consultato il 22 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/performing_bulk_recovery_for_recoveryplans.html.
94. Rubrik, "Recovery of a batch of virtual machines," consultato il 4 aprile 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
95. Rubrik, "Recovery of virtual machines," consultato il 16 aprile 2024, https://docs.rubrik.com/en-us/saas/saas/vs_recovery_vm.html.
96. Il data store recuperato è solitamente archiviato nel cluster Rubrik e non nell'ambiente di produzione.
97. Rubrik, "Recovery of a batch of virtual machines," consultato il 16 aprile 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
98. Dell, "Restore plan," consultato il 16 aprile 2024, https://infohub.delltechnologies.com/en-US/l/powerprotect-data-manager-protection-for-vmware-cloud-foundation-on-dell-emc-vxrail-1/restore-plan/.
99. Dell, "PowerProtect Data Manager overview," consultato il 16 aprile 2024, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-manager-deployment-best-practices-1/powerprotect-data-manager-overview-4/.
100. Dell, "PowerProtect Data Manager 19.9 Administration and User Guide," consultato il 16 aprile 2024, https://www.dell.com/support/manuals/en-us/enterprise-copy-data-management/pp-dm_19.9_ag/file-level-restore-of-a-powerprotect-backup-in-the-vsphere-client.
101. Dell, "Recovery Orchestration with PowerProtect Data Manager Overview," consultato il 16 aprile 2024, https://www.youtube.com/watch?v=po2oMnAg_x4.
102. Rubrik, "Quarantine files or objects," 24 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/quarantine.html.
103. Rubrik, "Downloading quarantined files for forensic analysis," 24 marzo 2024, https://docs.rubrik.com/en-us/saas/saas/downloading_quarantined_files_for_forensic_analysis.html.
104. Forrester, "The Total Economic Impact™ Of Dell PowerProtect Cyber Recovery," consultato il 16 aprile 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/the-total-economic-impact-dell-powerprotect-cyber-recovery.pdf.
105. Rubrik, "Workload recovery during an RSC service disruption," consultato il 16 aprile 2024, https://docs.rubrik.com/en-us/saas/saas/workload_recovery_during_rsc_outage.html.
106. Rubrik, "Rubrik CDM APIs and service account workflows," consultato il 16 aprile 2024, https://docs.rubrik.com/en-us/saas/saas/rubrik_apis_sa_workflows.html.
107. Rubrik, "Recoverable workloads during RSC service disruption," consultato il 16 aprile 2024, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.
108. Rubrik, "Workloads require third-party tools for recovery," consultato il 16 aprile 2024, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.

109. NIST, "Computer Security Resource Center Glossary: air gap," consultato il 29 luglio 2024, https://csrc.nist.gov/glossary/term/air_gap.

110. Dell, "Dell PowerProtect Cyber Recovery Solution Guide."

111. Dell, "Dell PowerProtect Cyber Recovery: Reference Architecture."

112. Adam Eckerle, "Debunking the Myths about Air Gaps," consultato il 14 marzo 2024, https://www.rubrik.com/blog/technology/2021/11/debunking-the-myths-about-air-gaps.

113. Rubrik, "Air-Gap, Isolated Recovery, and Ransomware - Cost vs. Value," consultato il 14 marzo 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/Air-Gap-Isolated-Recovery-and-Ransomware-Cost-vs.-Value.pdf.

114. Brian Williams, "Rubrik Air Gap and Immutability," consultato il 14 marzo 2024, https://vimeo.com/561870246.

115. Rubrik, "Retention locks in the Rubrik cluster," consultato il 18 marzo 2024, https://docs.rubrik.com/en-us/9.0/sg/security_guide/retention_locks_in_the_rubrik_cluster.html.

▶ Visualizza la versione originale in inglese di questo report

Questo progetto è stato commissionato da Dell Technologies.

Principled Technologies®

Facts matter.®