Migliora la cyber-resilienza e proteggi i dati dalle minacce informatiche di ransomware utilizzando un vault isolato, un software di analisi ML basato su AI e altro ancora

Con Dell Technologies PowerProtect Cyber Recovery e CyberSense

Con l'aumentare della frequenza degli attacchi informatici e l'evoluzione dei metodi di attacco, i piani di protezione dei dati devono adottare un approccio che protegga e analizzi tutti i componenti IT, dal più superficiale al più profondo. Dell PowerProtect Cyber Recovery può contribuire a proteggere i dati più critici e sensibili, garantendo al contempo un ripristino corretto in caso di attacco informatico o di un altro evento di interruzione.

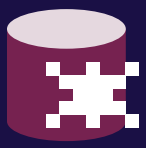
Dell PowerProtect Cyber Recovery è una soluzione di gestione, protezione e ripristino dei dati che aiuta le organizzazioni a proteggere i dati e le applicazioni da ransomware, attacchi informatici distruttivi ed eventi imprevisti. La soluzione utilizza un approccio multicopie, il che significa che dopo aver creato dei backup, li copia in uno storage isolato per la protezione e l'analisi. PowerProtect Cyber Recovery comprende molti componenti, tra cui uno o più vault di storage, che si trovano potenzialmente on-premise in un appliance PowerProtect DD (precedentemente noto come Data Domain) o nel cloud tramite Dell APEX Protection Storage for Public Cloud (precedentemente noto come DD Virtual Edition) software-defined. In entrambi i casi, il vault è un air gap operativo, ossia è isolato dall'ambiente di produzione, con potenziale air gap fisico il caso di ambiente on-premise e con air gap logico in caso di ambiente APEX. Ciò rende estremamente difficile per gli utenti malintenzionati o gli utenti non autorizzati accedere e compromettere le copie di backup.

PowerProtect Cyber Recovery include anche CyberSense, un motore di analisi della sicurezza intelligente completamente automatizzato e integrato che esegue automaticamente la scansione di dati, file, database e immagini nel vault per rilevare eventuali segni di danneggiamento dovuto a un attacco ransomware. CyberSense fornisce un'analisi completa dei contenuti; prende le osservazioni dai file da utilizzare come input per il suo modello di apprendimento automatico (ML) basato sull'intelligenza artificiale (AI) e rileva attività malevole che includono eliminazioni di massa, crittografia e altre modifiche sospette nell'infrastruttura core (tra cui Active Directory e DNS), file utente e database di produzione critici che potrebbero indicare ransomware o un attacco distruttivo. Quando CyberSense rileva modelli di danneggiamento, genera un avviso nel dashboard di PowerProtect Cyber Recovery che fornisce ulteriori informazioni sulla portata e sull'impatto dell'attacco.[1]

PowerProtect Cyber Recovery aiuta le organizzazioni a mitigare gli attacchi informatici, migliorare la resilienza dei dati con più copie di backup dei dati da posizioni separate, ridurre il downtime e mantenere la continuità aziendale. Questo report utilizza dati pubblicamente disponibili per evidenziare alcune caratteristiche e funzionalità chiave della protezione dei dati e presenta i nostri risultati da un'analisi competitiva di CyberSense.

Protegge i dati sensibili

Codifica i dati in-flight immutabili durante la replica di backup in vault isolati fisicamente e logicamente



Individua il danneggiamento della pagina SQL Server

CyberSense ha rilevato un'infezione che una soluzione concorrente non è riuscita a trovare

Identifica le copie di backup non danneggiate

CyberSense ha identificato la copia di backup non infetta più recente per il ripristino

Sicurezza

Dell PowerProtect Cyber Recovery offre diverse funzionalità di sicurezza per proteggere i dati critici da ransomware e altre minacce sofisticate, impedire agli utenti non autorizzati di accedere a informazioni sensibili e accelerare il ripristino in modo che le organizzazioni possano riprendere le normali operazioni.

Le caratteristiche e la funzionalità degli appliance PowerProtect DD sono fondamentali per la sicurezza, l'integrità e il ripristino offerti dalle soluzioni PowerProtect Cyber Recovery. Queste funzionalità comprendono:

1. **Inalterabilità**
   I dati non modificabili non possono essere modificati o eliminati, ma solo scritti. I sistemi DD possono scrivere backup non modificabili su entrambi i sistemi di produzione e nel cyber vault. Ciò significa che nel caso in cui un utente malintenzionato dovesse in qualche modo accedere al sistema di backup, non può modificare, eliminare o compromettere le copie protette esistenti.[2] Qualsiasi backup creato dal sistema DD nell'ambiente di produzione è immediatamente immutabile e disponibile per la copia nel vault per una maggiore sicurezza. La sezione successiva del presente report esamina maggiormente l'immutabilità.

2. **Retention Lock**
   La funzionalità DD Retention Lock consente di rendere i dati non modificabili per un periodo predeterminato. Una volta che la soluzione posiziona i dati sotto un retention lock, nessun utente o sistema può alterare, eliminare o modificare i dati fino alla scadenza del periodo di blocco.[3]

   Retention Lock dispone delle modalità di governance e conformità. La modalità di conformità consente ai clienti di soddisfare molti standard normativi. Una terza parte indipendente ha attestato che DD Retention Lock soddisfa i requisiti di storage specificati nelle norme SEC 17a-4(f)(2) e 240.18a-6(e)(2) e nella norma FINRA 4511(c).[4] Questa funzionalità può anche aiutare a supportare gli sforzi di un'organizzazione volti a rispettare la conformità alle norme FDA 21 cfr Part11, Sarbanes-Oxley Act, IRS 98025 e 97-22, ISO Standard 15489-1 e MoREQ2010.[5]

   Poiché gli utenti malintenzionati potrebbero tentare di aggirare Retention Lock modificando l'orologio di un sistema, azione che causerebbe l'eliminazione dei file prima del previsto, DD dispone di un orologio di sicurezza interno. Il sistema confronta regolarmente a livello di tempo gli orologi di sicurezza e di sistema. Se si verifica un disallineamento accumulato di due settimane tra i due in un unico anno di calendario, il sistema disabilita automaticamente il file system di DD (DDFS) per impedire l'accesso ai dati.[6]

3. **Crittografia dei dati in-flight con DDBoost**
   I dati in-flight possono rappresentare un rischio significativo per la sicurezza. DDBoost limita la quantità di dati in-flight consentendo al server di backup o al client dell'applicazione di inviare attraverso la rete all'appliance DD solo segmenti di dati univoci, anziché tutti i dati. Inoltre, le organizzazioni possono utilizzare il protocollo DDBoost con o senza certificati per l'autenticazione e la crittografia dei dati. I certificati offrono una funzionalità di trasporto dei dati più sicura. La crittografia in-flight consente alle applicazioni di crittografare il backup in-flight o ripristinare i dati su LAN dal sistema di protezione. Il cliente può sfruttare i Transport Layer Services (TLS) per crittografare la sessione tra il client e il sistema.[7]

4. **Sicurezza del sistema operativo DD (DD OS)**
   Le funzionalità di sicurezza del sistema DD si estendono anche al sistema operativo. DD OS implementa controlli di accesso personalizzati e restrizioni sulla shell Bash per scopi di sicurezza. La modalità shell Bash con restrizioni consente agli utenti di eseguire solo un set di comandi predefiniti necessari per i loro ruoli e per le attività di cui si occupano. DD OS migliora l'integrità dei dati bloccando comandi non definiti che apportano modifiche non autorizzate o non intenzionali al sistema.[8]

5. **Controllo degli accessi basato su ruoli (RBAC) e sicurezza del sistema di file DD (DDFS)**
   I sistemi DD utilizzano diverse misure per proteggere file e dati all'interno del file system. Innanzitutto, i sistemi DD forniscono RBAC, che consente agli amministratori di definire ruoli con privilegi specifici e assegnare utenti a tali ruoli. Solo gli utenti autorizzati con privilegi appropriati possono accedere all'appliance e ai relativi dati. In questo modo gli utenti hanno accesso solo alle funzioni e ai dati di cui hanno bisogno per eseguire le proprie attività, riducendo il rischio di accesso non autorizzato o di esposizione accidentale dei dati.

   DDFS utilizza anche l'hashing per la verifica dell'integrità dei dati. L'hash trasforma una determinata chiave o stringa di caratteri in un altro valore. L'appliance archivia blocchi di dati univoci in container di storage logici e il file system esegue l'hash dei blocchi di dati e dei container. Quando il sistema recupera i dati, ricalcola il valore hash dei dati in modo che corrisponda al valore hash archiviato in DDFS, fattore che aiuta a garantire che nulla abbia manomesso o danneggiato i dati.[9]

6. **Autorizzazione per doppio ruolo**
   Quando un'organizzazione abilita la modalità di conformità DD Retention Lock, il sistema DD fornisce ulteriore sicurezza amministrativa sotto forma di doppio accesso. In altre parole, l'amministratore del sistema e un secondo utente autorizzato (ad esempio, l'ufficiale di sicurezza) devono accedere insieme. Il meccanismo di doppio accesso della modalità di conformità DD Retention Lock funge da protezione contro eventuali azioni che potrebbero potenzialmente compromettere l'integrità dei file bloccati prima della scadenza del periodo di retention.[10]

7. **Data Invulnerability Architecture**
   DD OS fornisce verifica end-to-end, prevenzione e contenimento dei guasti, rilevamento e correzione continui dei guasti e ripristino del file system per proteggere dai problemi di integrità dei dati causati da malfunzionamenti hardware e software. Quando il sistema DD riceve richieste di scrittura dal software di backup, analizza innanzitutto un segmento di dati per la ridondanza calcolando l'impronta digitale per il segmento di dati e confrontandola con le impronte digitali esistenti archiviate nel sistema. Archivia solo segmenti di dati univoci e le relative impronte digitali su disco. Quindi DD legge continuamente i dati dal disco, ricalcola l'impronta digitale che legge a sua volta e garantisce che corrisponda all'impronta digitale sul disco. Il sistema DD esegue un processo di self-healing per ricostruire i dati danneggiati e ripristinarli allo stato corretto se il sistema rileva un danneggiamento durante questo processo (ad esempio, se ciò che legge non corrisponde a quanto scritto). Inoltre, il processo di self-healing aiuta a proteggere il sistema da altre modifiche che potrebbero influenzare l'integrità della piattaforma.

Immutabilità*

Rendere i backup immutabili e quindi read-only aiuta a garantire che un'organizzazione possa fidarsi di questi backup per il ripristino. Dal punto di vista operativo, l'immutabilità contribuisce a mantenere l'autenticità e l'affidabilità dei dati.

*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.

Come funziona

I sistemi DD offrono immutabilità nel modo in cui archiviano i dati utilizzando gli MTree. Gli MTree sono partizioni logiche del file system. Quando un'applicazione scrive dati in un MTree, il sistema DD utilizza una funzione chiamata Fast Copy per creare una copia point-in-time dell'MTree originale in un nuovo MTree. All'interno del nuovo MTree, DD applica Retention Lock per garantire che un utente o un processo non possa eliminare il nuovo MTree per la durata definita dal periodo di retention. Il nuovo MTree è una copia immutabile dei dati ed è indipendente dall'MTree originale.[11]

Le soluzioni PowerProtect Cyber Recovery usano anche la replica MTree per copiare copie di dati immutabili da un DD di produzione a un altro DD nel vault tramite il protocollo DDBoost.[12] Nella sincronizzazione iniziale tra i due DD, la soluzione copia tutti i dati nel DD del vault. Ogni sincronizzazione successiva copierà solo segmenti di dati nuovi e modificati. CyberSense, di cui parleremo più avanti in questo report, esegue la scansione di tutte le copie immutabili nel vault per rilevare potenziali danneggiamenti.

Approcci all'immutabilità

La necessità di eliminare i backup non modificabili è rara, ma è uno scenario che si verifica. Le organizzazioni possono potenzialmente incorrere in problemi di capacità e costi successivi dopo aver accumulato backup non modificabili che non possono eliminare. L'archiviazione dei backup può richiedere un'elevata quantità di capacità, che a sua volta impone costi operativi, di gestione e di monitoraggio continui oltre all'investimento hardware iniziale. L'eliminazione periodica di backup non modificabili può aiutare a risolvere questi problemi.

Come già sottolineato, Dell PowerProtect Cyber Recovery offre immutabilità grazie a Retention Lock e ad altri strumenti. Retention Lock offre una certa flessibilità poiché le due modalità, Compliance e Governance, offrono lievi modifiche al modo in cui i clienti possono implementare l'immutabilità. L'immutabilità significa che gli utenti o gli utenti malintenzionati non possono eliminare i backup, ma in alcuni casi, ad esempio per problemi di capacità di storage, PowerProtect Cyber Recovery consente ai clienti di eliminarli con la modalità Retention Lock - Governance.

In confronto a PowerProtect Cyber Recovery, come si posizionano le offerte simili di altre aziende? Abbiamo esaminato informazioni pubblicamente disponibili per Cohesity Cyber Recovery, Veeam, Rubrik e Veritas NetBackup. Ad eccezione di Cohesity Cyber Recovery, le soluzioni possono risiedere on-premise o off-premise (Cohesity è una soluzione basata su cloud supportata da AWS). La documentazione per le quattro soluzioni afferma di offrire immutabilità, ma è evidente che Rubrik e NetBackup presentano alcune differenze rispetto a PowerProtect Cyber Recovery.

Per Rubrik, gli amministratori possono eliminare i backup, ma non dal lato client e solo con determinati controlli. Inoltre, tutte le scritture sono del tipo "non sul posto", pertanto le nuove scritture non toccano mai i dati scritti in precedenza.[13]

Nonostante offra immutabilità, gli amministratori o gli utenti malintenzionati possono eliminare il blocco sui backup all'interno di uno storage compatibile con WORM di NetBackup. È quindi possibile eliminare l'immagine utilizzando il comando bpexpdate.[14]

Isolamento

L'isolamento dei dati si riferisce alla separazione e all'accesso limitato ai dati creati da barriere o confini per impedire l'accesso non autorizzato. L'isolamento utilizza connessioni di rete temporanee anziché connessioni persistenti.

L'isolamento dei dati aiuta i dati critici a rimanere sconnessi da una rete infetta, in cui un utente malintenzionato potrebbe tentare di modificare le configurazioni, eliminare i dati, modificare le policy o rilevare il traffico di rete per le credenziali utente. L'isolamento contribuisce inoltre a ridurre la superficie di attacco, offrendo ai malintenzionati minori opportunità di accesso e controllo. Inoltre, le organizzazioni possono limitare l'accesso solo al personale autorizzato, impedendo agli utenti non autorizzati di sovrascrivere i dati.

Oltre alle funzionalità indicate, PowerProtect Cyber Recovery può fornire isolamento fisico e logico, sotto forma di air gap operativi, per contribuire a proteggere i dati. PowerProtect Cyber Recovery può utilizzare un air gap fisico, in cui i dati di backup sono fisicamente disconnessi dalla rete di produzione e archiviati in una posizione isolata, così come un air gap logico, che si basa sui controlli dell'accesso alla rete per separare le copie di backup disconnesse logicamente dall'ambiente di produzione. Avere entrambi i tipi di air gap è prezioso perché un air gap logico da solo non può impedire a un utente interno con accesso di rete al vault di accedere e compromettere i dati.

Un PowerProtect DD on-premise fisicamente isolato potrebbe funzionare come vault in cui gli utenti o i sistemi dell'ambiente di produzione non possono accedere ai componenti e il vault è fisicamente scollegato dalla rete di produzione.[15] Eliminando l'accesso all'ambiente di ripristino dalla rete di produzione, un'organizzazione può ridurre la superficie di attacco. Come indicato, l'accesso ai dati isolati richiede credenziali di sicurezza separate e l'autenticazione a più fattori (MFA).[16]

Approcci all'isolamento

Gartner afferma che "gli ambienti di ripristino isolati (IRE) con vault di dati immutabili (IDV) forniscono il massimo livello di sicurezza e ripristino contro minacce interne, ransomware e altre forme di attacchi informatici".[17] Inoltre, notano che un "IRE con un IDV non sostituisce, ma integra, i sistemi di backup e ripristino di emergenza (DR) tradizionali fornendo una copia di backup terziaria non modificabile in un IRE dotato di tutti gli strumenti, i processi e le risorse per ripristinare i sistemi interessati".[18]

Esaminando le informazioni pubblicamente disponibili sulle soluzioni Cohesity, Veeam, Rubrik e Veritas, abbiamo riscontrato che ciascuna di esse ha un approccio IRE leggermente diverso da PowerProtect Cyber Recovery. Con la soluzione Dell, i clienti possono isolare fisicamente o logicamente i vault DD dalla produzione per mantenere il controllo e i piani di produzione separati dai vault stessi. Inoltre, PowerProtect Cyber Recovery automatizza gli air gap, funzione che non tutte le altre soluzioni offrono.

In base alla documentazione:

- Cohesity Cyber Recovery offre solo un air gap logico automatizzato dinamico per il vault FortKnox basato su AWS.[19]
- Veeam supporta un air gap logico per i provider di public e private cloud tramite Veeam Cloud Connect, ma non è automatizzato. Veeam offre anche il repository protetto Veeam, che funge da vault on-premise per la soluzione e che le organizzazioni possono configurare per avere un air gap fisico.[20]
- Rubrik non offre un air gap automatizzato per Rubrik Cloud Vault, ma i clienti possono aggiungerne uno logico tramite una partnership di terze parti con Microsoft.[21]
- I clienti NetBackup devono abilitare manualmente un air gap logico e hanno la possibilità di crearne uno fisico con una soluzione on-premise o off-premise.[22]

Come funziona

La Figura 1 mostra i percorsi di rete del vault di Cyber Recovery isolato. È bene notare che il vault non dispone di un percorso di gestione o controllo verso l'ambiente di produzione per ridurre la superficie di attacco.

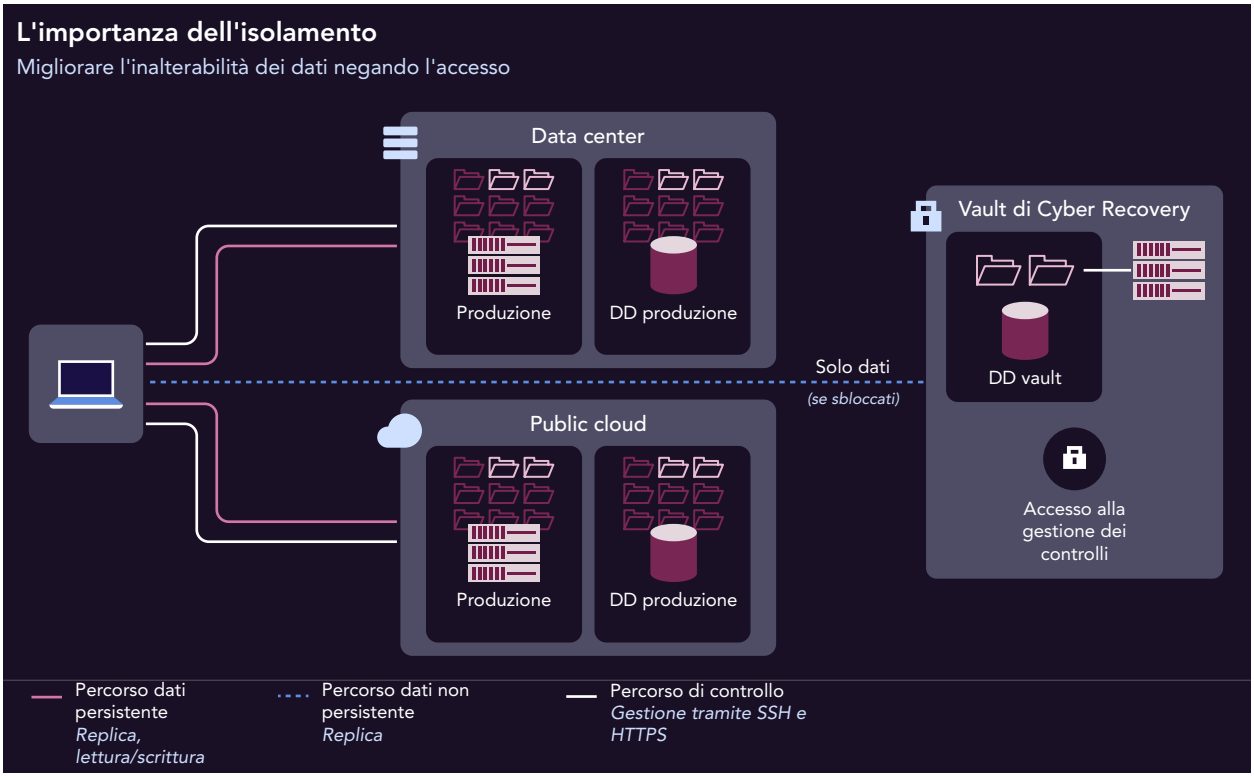


Figura 1. Architettura ad alto livello dei dati e del percorso di controllo del Cyber Recovery Vault. Fonte: Principled Technologies.

L'unica connessione richiesta per il vault di Cyber Recovery è un percorso dati per la sincronizzazione periodica dei dati. La sincronizzazione avviene quando la soluzione Cyber Recovery acquisisce i dati in brevi intervalli basati su policy per la replica.[23] Il documento PowerProtect Cyber Recovery Solution Guide afferma che "l'architettura della soluzione Cyber Recovery di base è costituita da una coppia di sistemi PowerProtect DD e dall'host di gestione di Cyber Recovery. In questa configurazione di base, il software Cyber Recovery, eseguito sull'host di gestione, abilita e disabilita l'interfaccia Ethernet di replica insieme ai contesti di replica sul sistema PowerProtect DD nel vault di Cyber Recovery per controllare il flusso di dati dall'ambiente di produzione all'ambiente vault".[24] Dell suggerisce ulteriori modi in cui le organizzazioni possono proteggere e isolare i percorsi dati. Abbiamo osservato Cyber Recovery sbloccare e bloccare il vault durante e dopo la replica nei nostri test.

Per l'implementazione fisica del vault, Dell consiglia di installare l'apparecchiatura del vault di Cyber Recovery in una stanza o gabbia dedicata con controlli degli accessi fisici. Questa stanza protetta deve disporre di un elenco degli accessi limitato con disconnessione della chiave o accesso con chiavi per due persone. Deve essere in atto la videosorveglianza dei punti di ingresso nella gabbia o nella stanza e delle apparecchiature. Per la massima sicurezza, il software Cyber Recovery deve essere accessibile solo tramite accesso fisico al server di gestione di Cyber Recovery e a una tastiera e un mouse associati".[25]

Con la separazione dei percorsi di gestione e di controllo, le opzioni di isolamento fisico e logico di Cyber Recovery si distinguono dalle altre soluzioni. Alcune soluzioni consentono l'accesso ai dati del vault da un'interfaccia dell'ambiente di produzione. In questo modo i dati del vault si trovano sulla stessa superficie di attacco dei dati di produzione, consentendo potenzialmente agli utenti malintenzionati di accedere alle copie di backup utilizzando credenziali compromesse.

CyberSense

La protezione dei dati richiede una strategia completa che offra sicurezza a ogni livello. Nonostante tutte le funzionalità di self-healing, sicurezza, immutabilità e isolamento di una soluzione Dell PowerProtect Cyber Recovery, attacchi meno evidenti potrebbero comunque entrare più in profondità nell'infrastruttura aziendale, ad esempio a livello di backup dei dati, rimanendo potenzialmente inosservati fino a quando i dati di produzione o un intero gruppo di utenti non sono stati danneggiati. Le soluzioni Dell PowerProtect Cyber Recovery offrono un'ultima linea di difesa contro gli attacchi informatici e un approccio efficiente per accelerare il ripristino tramite CyberSense. CyberSense è un engine di analisi che utilizza algoritmi di analisi ML basati sull'AI per eseguire la scansione e convalidare l'integrità dei backup nel vault e il contenuto utente dei file all'interno dei backup.

CyberSense viene eseguito all'interno del vault, isolato dall'ambiente di produzione. Monitora i file, le immagini delle VM e i database all'interno del vault per determinare se si è verificato un attacco informatico analizzando l'integrità dei dati. Una volta che la soluzione Cyber Recovery replica le copie di backup nel vault e applica la funzionalità Retention Lock, CyberSense esegue automaticamente la scansione delle copie, creando osservazioni point-in-time di file, database e infrastruttura core. L'engine di analisi esegue la scansione dell'intero contenuto dei file e di ogni pagina del database, non solo dei metadati. Laddove altre soluzioni cercano modifiche nelle soglie dei dati o nei metadati, CyberSense cerca all'interno del contenuto dei file per convalidare l'integrità dei dati. Queste osservazioni consentono a CyberSense di monitorare il modo in cui file e database cambiano nel tempo e di scoprire molti tipi avanzati di attacchi nascosti. CyberSense genera quindi analisi che rilevano modelli di danneggiamento che possono indicare attività di un utente malintenzionato, tra cui crittografia, eliminazione, creazione o offuscamento dei file e altro ancora.[26] Altre soluzioni portano l'analisi nel cloud, ampliando potenzialmente la superficie di attacco, mentre le organizzazioni possono scegliere di eseguire CyberSense on-premise o in una delle numerose opzioni cloud supportate da Cyber Recovery.

CyberSense combina oltre 200 analisi con osservazioni sui dati che diventano più utili nel tempo man mano che le stesse osservazioni aumentano. L'algoritmo ML utilizza informazioni su migliaia di infezioni da malware per individuare modelli di comportamento insoliti e distinguere l'attività dell'utente dal ransomware, riducendo al minimo falsi positivi e negativi. Attraverso la ricerca continua, l'algoritmo riceve una nuova formazione su elementi come le varianti di attacco. Inoltre, l'algoritmo ML riceve aggiornamenti basati sui dati reali dei clienti CyberSense esistenti.[27]

CyberSense supporta l'indicizzazione dei dati nei formati di backup su disco comuni di Dell, IBM, CommVault e Veritas.[28] Supportando formati di backup di altri vendor, Dell dimostra la volontà di soddisfare i clienti in base alle loro esigenze reali in termini di backup dei dati.

Abbiamo testato il software di analisi intelligente basato su ML di due soluzioni chiavi in mano per la protezione dei dati aziendali e il cyber recovery: CyberSense per Dell PowerProtect Cyber Recovery su un appliance di storage Dell PowerStore™ 7000T e uno strumento con funzionamento simile dalla piattaforma di gestione dati di un concorrente ("Vendor X") per un appliance di dimensioni simili.

Modalità di test

Abbiamo eseguito tutti i test da remoto e abbiamo avuto pieno controllo e accesso illimitato ai laboratori di test. La soluzione Dell comprensiva di CyberSense, applicazione di backup PowerProtect Data Manager, APEX Protection Storage (precedentemente nota come DD Virtual Edition) e PowerProtect Cyber Recovery, e quella del Vendor X si trovavano in un laboratorio di data center off-site.

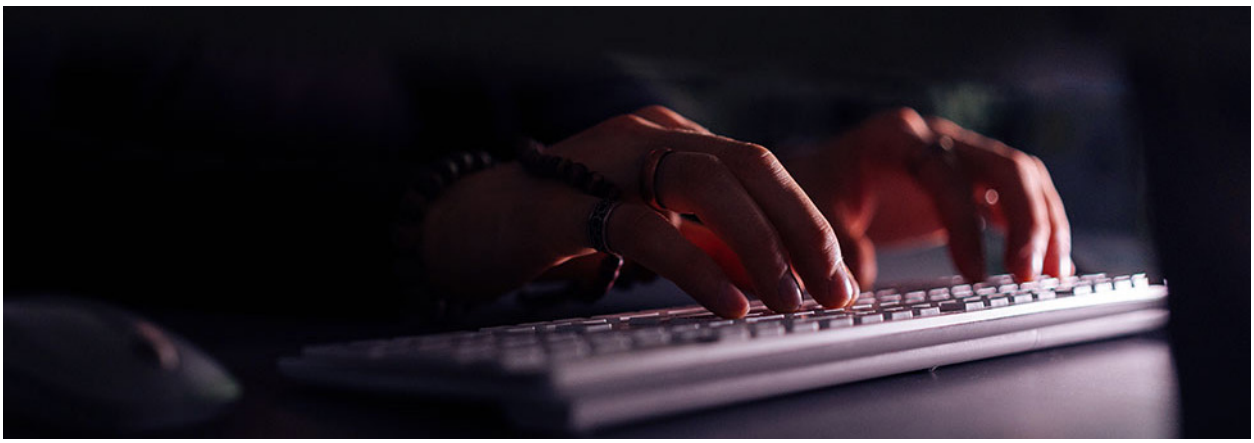
Per entrambe le soluzioni, abbiamo eseguito tre scenari di eventi dannosi basati su script che hanno come target i backup:

Figura 2. Scenari di test in cui operiamo. Fonte: Principled Technologies.

Per entrambe le soluzioni, i primi due scenari hanno seguito la stessa procedura generale. In primo luogo, abbiamo creato un backup completo di tutte le VM pulite sugli appliance di storage Dell PowerProtect Data Manager e del Vendor X, backup incrementali per la scansione e abbiamo verificato che la soluzione di destinazione non rilevasse una minaccia. Questo ci ha fornito un set di backup di base su cui eseguire gli script di attacco.

Successivamente, abbiamo eseguito lo script di simulazione ransomware su quattro VM con diversi sistemi operativi e vari tipi di applicazioni, abbiamo eseguito nuovi backup incrementali sull'appliance di destinazione e verificato che il software di analisi di destinazione rilevasse la minaccia di crittografia.

Per il terzo scenario (infezione di una pagina SQL Server), abbiamo seguito una procedura simile a quella degli altri due scenari, ma l'attenzione è stata concentrata sulle VM SQL e abbiamo utilizzato uno script di danneggiamento della pagina anziché uno script di crittografia. Abbiamo eseguito lo script su una singola VM.



Risultati

Scenario 1: Rilevamento di file criptati con nomi di file oscurati

Questo scenario ha simulato un evento dannoso che ha crittografato i file e offuscato i loro nomi, modificando i metadati del file oltre al suo contenuto. Questo tipo di attacco è in genere noto come ransomware, un evento di sicurezza in cui il software dannoso blocca l'accesso a un sistema informatico fino a quando il proprietario o l'utente del sistema non paga un importo predeterminato di denaro. Secondo la CISA (Cybersecurity and Infrastructure Security Agency) degli Stati Uniti, "[l]'impatto economico e reputazionale del ransomware e dell'estorsione dei dati si è dimostrato impegnativo e costoso per le organizzazioni di tutte le dimensioni durante l'interruzione iniziale e, a volte, durante il ripristino esteso".[29] L'utilizzo di un software di analisi intelligente per rilevare la crittografia nei backup può rafforzare la strategia di protezione dei dati di qualsiasi organizzazione, contribuire a proteggere informazioni preziose e sensibili e ridurre il potenziale di costosi tempi di inattività dovuti ad attacchi informatici.

Nei nostri test, entrambe le applicazioni di analisi intelligente hanno rilevato i file crittografati con nomi di file modificati. La soluzione del Vendor X ha necessitato di una baseline di 15 backup prima di rilevare infezioni (un backup completo e 14 backup incrementali), mentre CyberSense ha rilevato infezioni dopo un solo backup completo, il che significa che la soluzione del Vendor X ha richiesto 14 backup aggiuntivi rispetto a CyberSense.

Quando la soluzione del Vendor X ha avvisato dell'attività sospetta, ha indicato solo che qualche elemento aveva rimosso molti file e aggiunto un numero uguale di file, attività sospetta in base alla valutazione di entropia del backup.[30] La soluzione del Vendor X non ha indicato che i file erano stati crittografati o i nomi dei file modificati. Al contrario, Cyber Recovery con CyberSense ha avvisato che qualche elemento aveva crittografato e offuscato i nomi di file.

I risultati per il Vendor X potrebbero indicare un falso positivo. In altre parole, se ipotizziamo che un'organizzazione esegua backup giornalieri con la soluzione del Vendor X, potrebbe aver acquisito 14 giorni di file infetti prima del rilevamento delle anomalie. Al contrario, CyberSense ha necessitato di un solo backup baseline per avvisare in modo intelligente sull'infezione e sui relativi dettagli. In questa fase del nostro esempio, il ripristino con Cyber Recovery avviene dal vault isolato, garantendo all'organizzazione di non aver esposto la rete di produzione ai 14 backup infetti, come avrebbe fatto la soluzione del Vendor X.

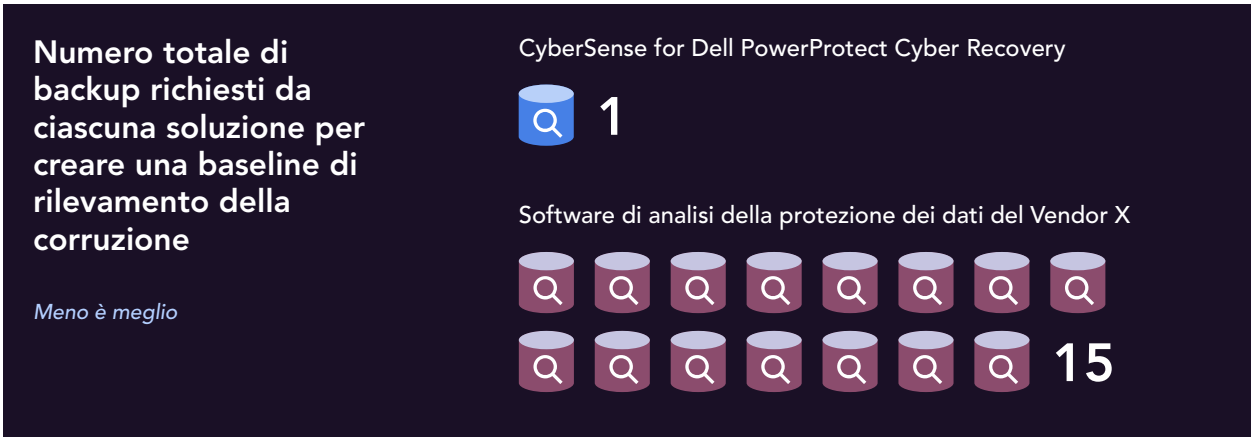


Figura 3. Numero di backup necessari per ciascuna soluzione per creare una baseline per il rilevamento del danneggiamento.
Fonte: Principled Technologies.

Scenario 2: Rilevamento di file criptati con nomi di file originali

Questo scenario era simile al primo, ma lo script conservava i nomi dei file originali dei file crittografati. Questa modifica non ha influito sui metadati dei file, ma solo sui file stessi. Un'azione come questa può essere un ransomware di tipo "timebomb", in cui l'attacco rimane inattivo per un periodo prima dell'attivazione. Il ransomware timebomb può eludere il rilevamento e i backup di destinazione, rendendo i backup infetti inutili quando l'organizzazione ne ha bisogno.[31] Senza modifiche nei metadati, il file potrebbe sembrare non infetto in superficie, contribuendo a mantenere nascosto l'attacco informatico dormiente.

Nei nostri test, entrambe le applicazioni di analisi intelligente hanno rilevato i file crittografati. Anche in questo caso, la soluzione del Vendor X ha necessitato di una baseline di 15 backup, inclusi 14 backup incrementali, prima di poter rilevare un'anomalia. CyberSense ha necessitato di una baseline composta da un solo backup completo prima di poter rilevare un'anomalia.

Come nel primo scenario, la soluzione del Vendor X ha avvisato solo del fatto che qualche elemento aveva modificato molti file, condizione sospetta in base alla valutazione di entropia del backup. Non ha indicato che tale elemento avesse crittografato i file, mentre Cyber Recovery con CyberSense ci ha fornito informazioni al riguardo. Il rilevamento del danneggiamento in tal modo significa che CyberSense sta esaminando il contenuto dei file, non solo i metadati a livello superficiale. Questo tipo di scansione aggiunge un altro livello di sicurezza per i backup e quindi per l'infrastruttura digitale o l'ambiente in generale. Si potrebbe suggerire che CyberSense sia una "vera" applicazione di analisi intelligente. Inoltre, le organizzazioni possono rilevare i danni prima con CyberSense, poiché la soluzione ha richiesto un numero significativamente inferiore di backup per creare una baseline. A seconda della pianificazione dei backup di un'organizzazione, potrebbe essere molto più veloce.

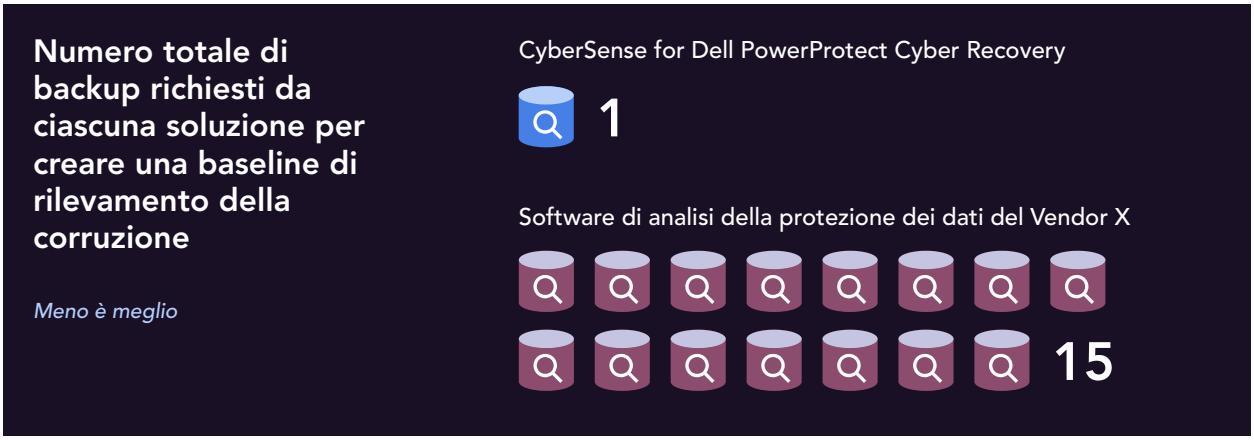


Figura 4. Numero di backup richiesti da ciascuna soluzione per rilevare il danneggiamento. Fonte: Principled Technologies.

Scenario 3: Rilevamento del danneggiamento della pagina SQL Server

Questo scenario ha simulato un evento dannoso che danneggiava una pagina SQL Server. In SQL Server, l'unità fondamentale di storage dei dati è la pagina e il database legge o scrive intere pagine di dati.[32] Anche in questo caso, questa modifica non ha influito sui metadati, ma solo sui file stessi. Questo tipo di attacco è comunemente noto come SQL injection, in cui gli autori di attacchi hanno come target le applicazioni basate sui dati SQL tramite l'inserimento di codice dannoso nelle istruzioni SQL tramite input di pagina web.[33] Anche se infetti, i database possono continuare a essere eseguiti. Oltre al furto di dati, le pagine SQL Server danneggiate possono causare problemi di integrità dei dati, perdita di questi ultimi e interruzioni della funzionalità del database. Questi risultati possono danneggiare la reputazione di un'organizzazione, interrompere i flussi di lavoro operativi, portare a perdite finanziarie, e persino comportare una responsabilità legale.

Sebbene CyberSense e la soluzione del Vendor X abbiano entrambe rilevato la crittografia nei primi due scenari, solo CyberSense ha eseguito una scansione sufficientemente approfondita da rilevare il danneggiamento nella pagina SQL Server in questo terzo scenario. Ciò dimostra che, sebbene le due soluzioni offrano capacità di rilevamento simili per certi livelli, CyberSense offre una scansione più approfondita dei backup per applicazioni basate su SQL Server potenzialmente business-critical. In questo modo, CyberSense aggiunge un livello di resilienza di sicurezza con scansioni più approfondite e una protezione più completa.

SQL Server supporta molte applicazioni nei settori finanziario, retail, sanitario e così via. Poiché SQL Server può fungere da back-end dell'architettura di sviluppo, un attacco a SQL Server può causare downtime, interrompere le operazioni e potenzialmente minacciare le entrate generate da queste applicazioni.

Restore e ripristino con Dell PowerProtect Cyber Recovery

La strategia di cyber-resilienza di Dell offre un'ampia gamma di funzionalità di ripristino. Queste opzioni di ripristino includono funzionalità comuni del settore, come l'accesso istantaneo o il ripristino tradizionale dai backup immutabili mantenuti in produzione. Inoltre, Dell offre funzionalità di ripristino esclusive dalla soluzione PowerProtect Cyber Recovery. Poiché PowerProtect Cyber Recovery mantiene le copie in isolamento ed esegue la scansione per verificarne l'integrità con CyberSense, le organizzazioni possono accedere alle copie immediatamente dopo un attacco e utilizzarle per avviare i passaggi di ripristino o i ripristini immediati su piattaforme di ripristino alternative, come camere bianche.

È opportuno confrontare questo caso d'uso immediato con un'organizzazione che può accedere ai dati solo in produzione o nel public cloud. L'organizzazione non può accedere in modo sicuro ai dati archiviati nell'area compromessa fino a quando non ha determinato e risolto la root cause, ha chiuso la persistenza degli attori malintenzionati, ha acquisito immagini forensi per gli assicuratori e il loro ufficio legale, ha analizzato nuovamente i dati e dispone di un'infrastruttura disponibile sufficiente (ad, DNS) per accedere all'infrastruttura di backup. Questo processo potrebbe richiedere giorni o settimane in base all'ambito e al livello di sofisticazione dell'attacco.

Come funziona

Durante la normale produzione, PowerProtect Cyber Recovery crea automaticamente dei punti di ripristino per il ripristino e l'analisi della sicurezza. In caso di attacco informatico, Cyber Recovery utilizza le sue procedure di restore e ripristino automatizzate e tali punti di ripristino per riportare online i sistemi business-critical. CyberSense e i report forensi aiutano i team di sicurezza informatica e ripristino a diagnosticare l'impatto dell'attacco. Una volta che l'ambiente di produzione è pulito e pronto per il ripristino, Cyber Recovery fornisce gli strumenti e la tecnologia che eseguono il ripristino effettivo dei dati.

A seguito di un attacco informatico, vengono messe in gioco diverse metriche di protezione dei dati per determinare la velocità di ripristino (il tempo di ripristino informatico o CRT) e il punto in cui gli utenti possono tornare dopo un attacco distruttivo (il punto di ripristino informatico o CRP). Per una soluzione Cyber Recovery, queste metriche includono quanto segue:

- **Destruction Detection Objective (DDO):** si tratta di una finestra continua basata sulla quantità di tempo tra un attacco informatico e il suo rilevamento. L'analisi e altri meccanismi di Cyber Recovery devono funzionare entro questo periodo.
- **Destruction Assessment Objective (DAO):** si tratta della quantità di tempo assegnata al team di sicurezza informatica in seguito a un'incursione per determinare l'ambito del danno e le potenziali risposte.
- **Intervallo di sincronizzazione di Cyber Recovery:** è la frequenza con cui la soluzione Cyber Recovery copia i dati dall'ambiente di produzione al vault. I tempi si basano su un RPO (Recovery Point Objective) stabilito in precedenza per la soluzione. Il periodo di conservazione delle copie varia a seconda della soluzione, ma di solito si aggira tra una settimana e un mese.
- **Numero di copie dei dati di Cyber Recovery:** numero di copie dei dati conservate nel vault di Cyber Recovery. Se associata all'intervallo di sincronizzazione, questa metrica fornisce una misura approssimativa di quanto indietro nel tempo un'organizzazione possa ripristinare i dati, ad esempio, sette copie abbinate a un intervallo di 24 ore consentono agli utenti di ripristinare i dati fino a una settimana fa.

Oltre ai requisiti di recupero, il tipo di dati che la soluzione protegge può aiutare a determinare l'intervallo di sincronizzazione dei dati e il tempo di conservazione. Secondo il documento Cyber Recovery Solution Guide, per ottenere la massima flessibilità di ripristino, gli utenti possono classificare i dati protetti dalla soluzione in uno dei seguenti flussi di backup:[34]

- backup di file binari ed eseguibili, tra cui distribuzioni del sistema operativo di base e build di applicazioni;
- backup completi di applicazioni e file system, tra cui immagini e dati specifici dell'applicazione.

Questi flussi di backup separati portano a due diverse strategie di ripristino:

1. **Ripristino dei file binari di dati e applicazioni nel vault di Cyber Recovery:**
   La soluzione identifica i punti di ripristino utilizzabili, insieme al malware e alla posizione in cui è persistente, e decide se ripulire il malware dall'immagine di backup o ricostruirlo utilizzando le copie del vault di Cyber Recovery. Dopo aver applicato le patch di sicurezza, la soluzione ripristina i dati su un host di ripristino utilizzando il runbook DR per l'applicazione, quindi determina se il processo di ripristino ha eliminato gli effetti del malware. Esegue quindi un test sull'applicazione utilizzando l'elaborazione del vault e pulisce o ricrea l'immagine dell'ambiente di produzione. Infine, Cyber Recovery connette l'host di ripristino alla produzione e copia l'applicazione e i dati di nuovo nell'ambiente di produzione. La Figura 5 mostra questo processo.

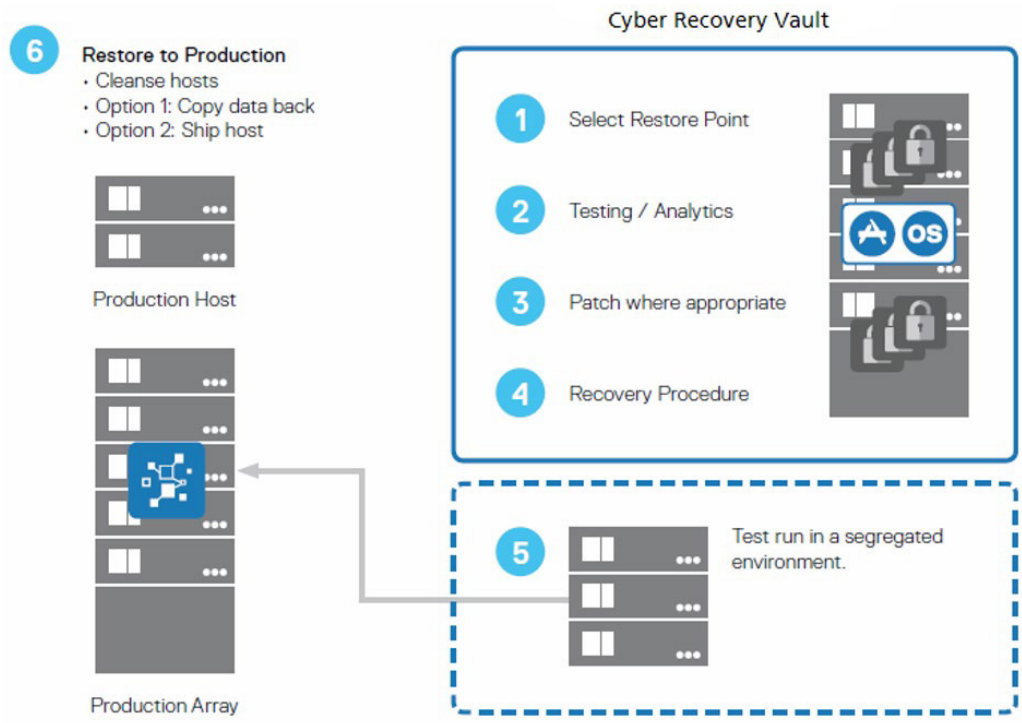


Figura 5. Processo per il ripristino dei file binari di dati e applicazioni. Fonte: Dell Technologies.[35]

2. **Ricostruzione completa dal vault di Cyber Recovery:**
   In questo approccio, la soluzione Cyber Recovery riformatta i sistemi di produzione in base al livello di danno determinato dalla valutazione forense durante la risposta agli incidenti. La soluzione ricostruisce quindi i file binari tramite copie nel vault di Cyber Recovery e applica le patch di sicurezza disponibili. Infine, ripristina le copie appropriate di applicazioni, dati e file di configurazione nell'ambiente di produzione utilizzando i runbook di DR associati per l'applicazione. La Figura 6 mostra questo processo.

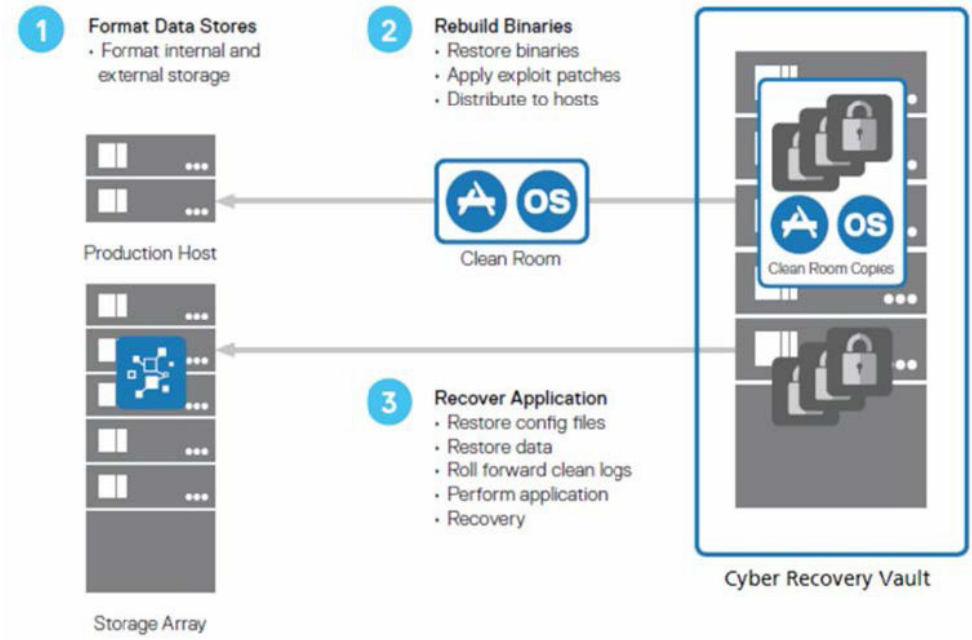


Figura 6. Processo per la ricostruzione completa dal vault di Cyber Recovery. Fonte: Dell Technologies.[36]

Le soluzioni Cyber Recovery includono host di ripristino fisici o virtuali (o entrambi) che il software Cyber Recovery può utilizzare per il ripristino. Questi host includono sia un server di ripristino delle applicazioni di backup, che è un server designato in cui vengono ripristinati l'applicazione di backup e il catalogo delle applicazioni di backup, sia un server di ripristino delle applicazioni. Le organizzazioni possono implementare più server a seconda dei requisiti di ripristino della soluzione. Il software Cyber Recovery può esporre le copie dei dati del sandbox (un ambiente di test per l'esecuzione sicura di software nuovi o non testati) a qualsiasi host per eseguire ripristini dei dati all'interno del vault, ad esempio dati del file system, dati di backup IBM, CommVault e Veritas o dati protetti da Dell NetWorker, Dell Avamar, un PowerProtect DP Series Appliance o dal software Dell PowerProtect Data Manager. Dopo il ripristino di un'applicazione di backup all'interno del vault, la soluzione può ripristinare tali dati in host di ripristino aggiuntivi nel vault.

Le organizzazioni dimensionano il server di ripristino delle applicazioni di backup in anticipo, in modo che gli utenti possano ripristinare tutte le applicazioni di backup protette dalla soluzione Cyber Recovery. Analogamente, il server di ripristino delle applicazioni è un server designato in cui la soluzione ripristina le applicazioni. Alcune applicazioni potrebbero richiedere ai clienti di ripristinare prima altre applicazioni dipendenti. L'infrastruttura all'interno del vault può supportare il ripristino dell'applicazione di produzione più grande protetta dalla soluzione.

Conclusioni

Durante la creazione di un piano di protezione dei dati, le organizzazioni devono prendere in considerazione molti vettori di attacco. Tale piano include la protezione di tutti i dati, ma soprattutto dei dati critici essenziali per le operazioni. PowerProtect Cyber Recovery isola i dati critici e garantisce il ripristino corretto dei dati in caso di attacco informatico. Cyber Recovery utilizza l'analisi basata su ML in CyberSense per determinare l'integrità dei dati nel vault e identificare i dati di backup puliti per il ripristino. Nel nostro test, abbiamo rilevato che PowerProtect Cyber Recovery ha individuato un'infezione nelle pagine del database SQL, condizione che la soluzione della concorrenza non era stata in grado di rilevare. PowerProtect Cyber Recovery ha richiesto anche un numero inferiore di backup rispetto alla soluzione del Fornitore X per determinare il danneggiamento dei dati. Oltre a tutti questi e altri aspetti, la soluzione Cyber Recovery offre molte opzioni di ripristino basandosi su dati non compromessi provenienti dal vault per un ritorno efficiente e ottimale alle operazioni.

---

1. Dell, "CyberSense® for PowerProtect Cyber Recovery", consultato l'8 settembre 2023, https://www.delltechnologies.com/asset/en-in/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
2. Dell, "Dell PowerProtect Cyber Recovery Solution Guide", consultato il 23 agosto 2023, 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. Cohasset Associates, Inc, "Dell Technologies PowerProtect DD and DDVE – Compliance Assessment: SEC 17a-4(f), SEC 18a-6(e) and FINRA 4511(c)", consultato il 27 ottobre 2023, https://infohub.delltechnologies.com/section-assets/cohasset-dell-powerprotect-dd-compliance-assessment.
5. Dell, "Data Domain: Retention Lock Frequently Asked Questions", consultato il 12 settembre 2023, https://www.dell.com/support/kbdoc/en-us/000079803/data-domain-retention-lock-frequently-asked-questions-faq.
6. Dell, "Data Domain: Retention Lock Frequently Asked Questions".
7. Dell, "Encryption types offered by DD series encryption appliance", consultato l'8 settembre 2023, https://infohub.delltechnologies.com/l/powerprotect-dd-series-appliances-encryption-software-1/encryption-types-offered-by-dd-series-encryption-appliance.
8. Dell, "Dell EMC Data Domain – Security Configuration Guide", consultato l'11 settembre 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu91808.pdf.
9. Dell, "Role Based Access Control (RBAC) in Data Domain", consultato l'11 settembre 2023, https://www.dell.com/community/en/conversations/data-domain/role-based-access-control-rbac-in-data-domain/647f70a9f4ccf8a8dee30f99.
10. Dell, "Dell EMC Data Domain – Security Configuration Guide".
11. Dell, "MTree replication", consultato l'11 settembre 2023, https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3.

12. Veeam, "Dell EMC Data Domain - DataDomain MTree overview and Limits", consultato l'11 settembre 2023, https://bp.veeam.com/vbr/2_Design_Structures/D_Veeam_Components/D_backup_repositories/datadomain.html
13. Chris Wahl, "Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture," consultato il 13 dicembre 2023, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
14. Veritas, "NetBackup™ Security and Encryption Guide", consultato il 13 dicembre 2023, https://www.veritas.com/support/en_US/doc/21733320-149123528-0/v143394540-149123528.
15. Principled Technologies, "Dell EMC Cyber Recovery protected our test data from a cyber attack", consultato il 21 agosto 2023, http://facts.pt/rkew01n.
16. Dell, "Dell PowerProtect Cyber Recovery", consultato il 12 settembre 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/isolated-recovery-solution-overview.pdf.
17. Jerry Rozeman e Michael Hoeck, "Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware", consultato il 14 dicembre 2023, https://www.gartner.com/doc/reprints?id=1-27MOHCBD&ct=211011&st=sb.
18. Jerry Rozeman e Michael Hoeck, "Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware".
19. Nikitha Okmar, "Going Beyond the Air Gap - Data Isolation and Recovery for the Modern era", consultato il 13 dicembre 2023, https://www.cohesity.com/blogs/going-beyond-the-air-gap-data-isolation-and-recovery-for-the-modern-era/.
20. Marco Horstmann, "How to Protect your data from ransomware and Encryption Trojans", consultato il 13 dicembre 2023, https://www.veeam.com/blog/how-to-protect-against-ransomware-data-loss-and-encryption-trojans.html.
21. Rubrik, "REST Easy with immutable, off-site data storage", consultato il 13 dicembre 2023, https://www.rubrik.com/products/rubrik-cloud-vault.
22. Veritas, "NetBackup Isolated Recovery Environment", consultato il 13 dicembre 2023, https://www.veritas.com/content/dam/www/en_us/documents/solution-overview/SO_flex_appliance_netbackup_ire_solution_V1543.pdf.
23. CSI Group, "Dell Cyber Recovery Vault (overview by CSI)", consultato il 23 agosto 2023, https://youtu.be/ej5nZzWNRM0.
24. Dell, "Dell PowerProtect Cyber Recovery Solution Guide."
25. Dell, "Dell PowerProtect Cyber Recovery Solution Guide."
26. Dell, "CyberSense® for PowerProtect Cyber Recovery."
27. Dell, "CyberSense® for Dell PowerProtect Cyber Recovery – Powered by Index Engines", consultato il 13 settembre 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/cybersense-for-dell-powerprotect-cyber-recovery-whitepaper.pdf.
28. Index Engines, "CyberSense for Dell Cyber Recovery", consultato il 25 settembre 2023, https://indexengines.com/csmatrix.
29. CISA, "#StopRansomware Guide", consultato il 1° agosto 2023, https://www.cisa.gov/stopransomware/ransomware-guide.
30. "In security, most people use Shannon Entropy—a specific algorithm that returns a value between 0 and 8. The higher the number, the more random the data, and many times, a higher value means that the data is either packed or encrypted". Mueller, Clint, "How to Use Entropy Analysis in Penetration Testing", consultato il 28 agosto 2023, https://www.schellman.com/blog/cybersecurity/penetration-testing-methods-entropy.
31. Cooper, Steven, "How to Protect Your Backups from Ransomware in 2023", 1° agosto 2023, https://www.comparitech.com/net-admin/protect-backups-from-ransomware/.
32. Microsoft, "Pages and Extents Architecture guide", consultato il 3 agosto 2023, https://learn.microsoft.com/en-us/sql/relational-databases/pages-and-extents-architecture-guide?view=sql-server-ver16.
33. W3 Schools, "SQL Injection", consultato il 3 agosto 2023, https://www.w3schools.com/sql/sql_injection.asp.
34. Dell, "Dell PowerProtect Cyber Recovery Solution Guide."
35. Dell, "Dell PowerProtect Cyber Recovery Solution Guide."
36. Dell, "Dell PowerProtect Cyber Recovery Solution Guide."

Leggi le basi scientifiche di questo report ▶

▶ La versione originale in inglese di questo report è disponibile all'indirizzo https://facts.pt/64FU3b2

Principled Technologies®

Facts matter.®

Principled Technologies è un marchio registrato di Principled Technologies, Inc.
Tutti gli altri nomi di prodotto sono marchi dei rispettivi proprietari.
Per ulteriori informazioni, consultare le basi scientifiche di questo report.

Questo progetto è stato commissionato da Dell Technologies.