DELL Technologies

Solution brief

Dell PowerProtect Cyber Recovery

Protezione moderna e resiliente dei dati critici da ransomware e attacchi informatici distruttivi.

PERCHÉ SCEGLIERE CYBER RECOVERY?

L'obiettivo degli attacchi informatici è quello di compromettere i dati più importanti, inclusi i backup. Proteggere e ripristinare i dati critici secondo un approccio sicuro orientato all'integrità è fondamentale per riprendere le normali operazioni di business dopo un attacco informatico.

Ecco i componenti di una soluzione cyber-resiliente:

Immutabilità dei dati
Creazione di copie di dati non modificabili per preservarne l'integrità e la riservatezza con livelli di sicurezza e controlli.

Isolamento e governance dei dati
Ambiente di ripristino isolato scollegato dalle reti aziendali e di backup con accesso utente con limitazioni elevate.

Copia automatizzata dei dati e air gap Creazione di copie di dati non modificabili all'interno di un vault digitale protetto e processi che generano un air gap operativo tra l'ambiente di produzione/backup e il vault.

Analisi intelligente
Controlli di integrità automatizzati utilizzando l'apprendimento automatico basato sull'AI e l'indicizzazione completa dei contenuti con potenti analisi all'interno della sicurezza del vault per stabilire se i dati sono stati colpiti da malware.

Ripristino e correzione
Flussi di lavoro e strumenti per eseguire il ripristino dopo un incidente utilizzando processi di ripristino dinamici e procedure DR esistenti.

Pianificazione e progettazione della soluzione Istruzioni per la selezione di data set, applicazioni e altri asset critici al fine di stabilire gli obiettivi RTO/RPO e semplificare il ripristino.

La sfida: gli attacchi informatici sono il nemico delle aziende con un approccio basato sui dati.

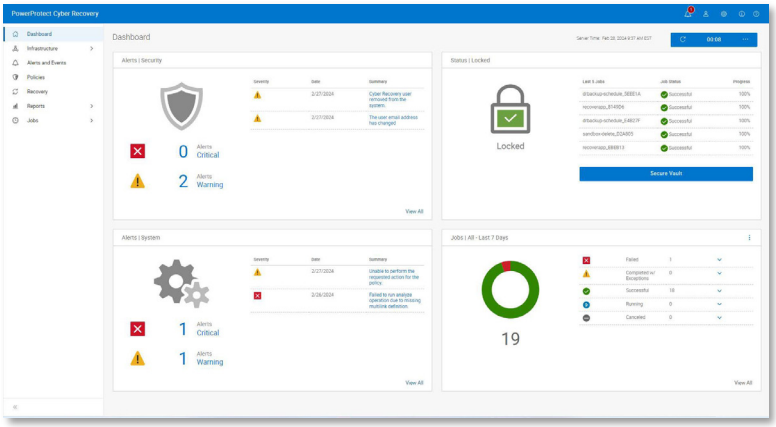
I dati sono la valuta dell'economia digitale e un asset vitale che deve essere salvaguardato, mantenuto riservato e facilmente accessibile. Il mercato globale moderno dipende dal flusso continuo di dati attraverso reti interconnesse. Le iniziative di Digital Transformation e il crescente utilizzo dell'AI generativa aumentano l'esposizione di informazioni sensibili.

In questo modo, i dati delle organizzazioni diventano un obiettivo appetibile dei criminali informatici, il cui scopo è lucrare a spese degli utenti. A prescindere dal settore o dalle dimensioni dell'azienda, gli attacchi informatici espongono continuamente organizzazioni ed enti pubblici a compromissione dei dati, perdita di entrate dovuta a downtime, danno alla propria reputazione e ingenti sanzioni dovute al mancato rispetto delle normative.

Disporre di una strategia di cyber-resilienza è divenuto un requisito fondamentale per i leader aziendali e governativi, eppure molte organizzazioni non hanno fiducia nelle proprie soluzioni di protezione dei dati. Il Global Data Protection Index ha rilevato che il 79% dei responsabili delle decisioni IT è preoccupato della possibilità di dover affrontare un evento di interruzione nei prossimi 12 mesi e il 75% teme che le misure di protezione dei dati adottate nella propria organizzazione non siano sufficienti per fronteggiare le minacce malware e ransomware[1].

La soluzione: Dell PowerProtect Cyber Recovery

Per ridurre i rischi per il business associati agli attacchi informatici e creare un approccio più cyber-resiliente alla protezione dei dati, è possibile modernizzare e automatizzare le strategie di ripristino e continuità aziendale, oltre a sfruttare gli strumenti intelligenti più recenti per rilevare eventuali minacce informatiche e difendersi.



Dell PowerProtect Cyber Recovery offre una soluzione di protezione comprovata, moderna, resiliente e intelligente per isolare i dati critici, identificare le attività sospette e accelerare il ripristino dei dati, semplificandolo in modo intelligente, per riprendere rapidamente le normali operazioni aziendali.

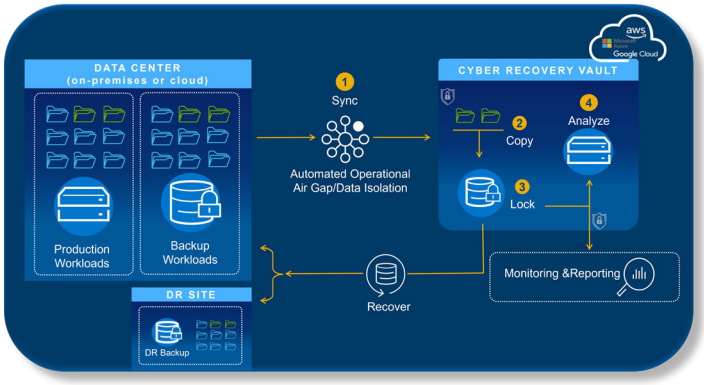
PowerProtect Cyber Recovery: immutabilità, isolamento e intelligenza

Immutabilità: PowerProtect Data Domain

PowerProtect Data Domain è la base di Dell PowerProtect Cyber Recovery. Con molteplici livelli di sicurezza Zero Trust, fornisce copie di backup non modificabili per garantire l'integrità e la riservatezza dei dati. Funzionalità come Root of Trust hardware, avvio protetto, crittografia, blocco delle retention, accessi basati sui ruoli e autenticazione a più fattori garantiscono la possibilità di ripristino dei dati.

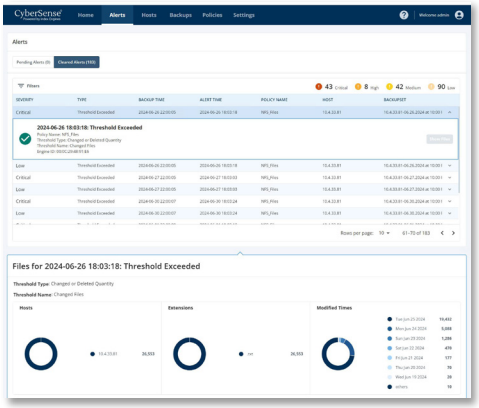
Isolamento: vault di Cyber Recovery

Il vault di PowerProtect Cyber Recovery è un ambiente di ripristino isolato che offre diversi livelli di protezione per fornire resilienza contro gli attacchi informatici, anche in caso di minaccia interna. L'air gap operativo sposta automaticamente (sincronizza) le copie dei dati di backup critici dalla superficie di attacco degli ambienti di produzione, inclusi open system e mainframe, in un vault fisicamente isolato. Una volta sincronizzati i dati critici con il vault, viene creata automaticamente una copia non modificabile per evitare che i dati vengano modificati. Con gestione, rete e servizi dedicati indipendenti dall'ambiente di produzione, sono necessarie credenziali di sicurezza separate e autenticazione a più fattori per accedere ai dati per le operazioni di ripristino e test.



Intelligence - CyberSense®

PowerProtect Cyber Recovery è la prima soluzione che integra completamente CyberSense® per ripristini più intelligenti contro le minacce informatiche, il tutto all'interno della sicurezza del vault di Cyber Recovery. CyberSense va oltre le soluzioni basate solo sui metadati: con l'analisi completa, rileva il danneggiamento dei dati dopo un attacco con il 99,99% di accuratezza[2] e facilita il recupero rapido e intelligente. CyberSense sfrutta i backup di dati non modificabili per osservare come i dati cambiano nel tempo e utilizza l'apprendimento automatico basato sull'AI per rilevare segni di danneggiamento indicativi di un attacco ransomware. CyberSense rileva inoltre eliminazioni di massa, crittografia parziale e totale e altri cambiamenti sospetti nell'infrastruttura core (ad esempio Active Directory, DNS e così via) nei file utente e nei database risultanti da attacchi sofisticati. È possibile creare avvisi di soglia personalizzati e, se vengono rilevati segni di danneggiamento, il dashboard degli avvisi e i report forensi post-attacco facilitano una rapida diagnosi della portata e dell'impatto dell'attacco, inclusa l'identificazione di una copia pulita dei dati per ripristinare i sistemi critici.



PowerProtect Cyber Recovery: opzioni di distribuzione

Cyber Recovery in ambienti ibridi e multi-cloud

I dati critici possono trovarsi in molte posizioni diverse all'interno di un'azienda, on-premise, collocati in data center diversi o a livello globale in più cloud e regioni. Indipendentemente dalla posizione, i dati devono essere protetti e non inclusi quando è necessario eseguire il ripristino da attacchi informatici.

PowerProtect Cyber Recovery è disponibile ed eseguibile tramite marketplace di public cloud per *AWS, Microsoft Azure* e *Google Cloud* per fornire un accesso rapido alla protezione dei dati in un vault di Cyber Recovery nel cloud. PowerProtect Cyber Recovery automatizza la sincronizzazione dei dati critici tra i sistemi di produzione e il vault di Cyber Recovery nel public cloud. A differenza delle soluzioni di backup standard basate su cloud, l'accesso alle interfacce di gestione è bloccato dai controlli di rete e richiede credenziali di sicurezza separate, nonché l'autenticazione a più fattori per l'accesso. La diffusione e la duplicazione dei dati su più cloud può comportare nuovi rischi per la sicurezza e la conformità, potenziali problemi di sincronizzazione e un aumento dei costi delle risorse. Questo approccio può anche ridurre la visibilità nei vari ambienti, rendendo la protezione insufficiente per le minacce informatiche in costante evoluzione.

Dell PowerProtect Cyber Recovery con Data Service Dell MultiCloud, con tecnologia Faction, rende i dati accessibili contemporaneamente ai provider di public cloud senza compromettere la sicurezza, offre la possibilità di scegliere qualsiasi provider di cloud e di evitare di vincolarsi a un vendor. Questo servizio di vaulting di dati protetto è un vault dotato di air gap logico, basato su un'infrastruttura sicura e multi-cloud che protegge i dati critici dagli attacchi informatici. Quando è necessario il ripristino dei dati, è possibile scegliere di eseguirne il restore dal vault ad AWS, Microsoft Azure, Google Cloud, Oracle Cloud o di nuovo all'ambiente locale.

Dell APEX Protection Storage All-Flash per Cyber Recovery

Mentre i dati critici continuano a crescere, la capacità di eseguire il ripristino in modo rapido ed efficiente da un evento informatico è fondamentale per garantire la continuità aziendale e la cyber-resilienza. Le organizzazioni che stanno espandendo la gestione dei dati critici devono eccellere nel recupero dei dati da ambienti di ripristino isolati, come il vault di Cyber Recovery. Dell APEX Protection Storage All-Flash, basato su una versione software-defined di PowerProtect Data Domain, offre una soluzione di ripristino dopo un attacco informatico semplificata, efficiente dal punto di vista energetico e a costi contenuti, dotata di funzionalità avanzate di analisi CyberSense e di ripristino rapido per soddisfare gli SLA delle organizzazioni. Utilizzando meno hardware, spazio ed energia, le organizzazioni possono migliorare la velocità di accesso ai dati, incrementare l'efficienza operativa e garantire l'integrità dei dati, con conseguente riduzione del downtime e dei costi complessivi di manutenzione.

PowerProtect Cyber Recovery: ripresa delle attività

Ripristino e correzione

PowerProtect Cyber Recovery esegue procedure automatizzate di restore e ripristino per riportare online i sistemi business-critical in modo rapido e sicuro. Il ripristino è integrato con il processo di risposta agli incidenti. Quando si verifica un evento, il team di risposta agli incidenti analizza l'ambiente di produzione per determinare la root cause dell'evento. CyberSense fornisce report forensi post-attacco per comprenderne la profondità e l'ampiezza e fornisce un elenco degli ultimi backup set validi prima del danneggiamento. Quindi, quando la produzione è pronta per il ripristino, Cyber Recovery fornisce gli strumenti di gestione e la tecnologia che esegue il ripristino effettivo dei dati.

Pianificazione e progettazione delle soluzioni

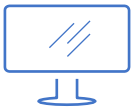
Grazie ai Dell Professional Services per Cyber Recovery è possibile stabilire quali sistemi business-critical proteggere e creare mappe delle dipendenze per le applicazioni e i servizi associati, oltre all'infrastruttura necessaria per ripristinarli. Questi servizi prevedono anche la definizione dei requisiti di ripristino e delle alternative di progettazione. Inoltre, identificano le tecnologie per analizzare, mettere in hosting e proteggere i dati, insieme alla creazione di un business case e alla definizione delle tempistiche di implementazione.

Conclusioni

Iniziative di settore come Sheltered Harbor utilizzano PowerProtect Cyber Recovery per proteggere i clienti, gli istituti finanziari e la fiducia del pubblico nel sistema finanziario degli Stati Uniti in caso di un attacco informatico che causi il guasto di sistemi critici, inclusi i backup. Con migliaia di clienti, Cyber Recovery con CyberSense offre fiducia ai leader aziendali e ha dimostrato di accelerare il ripristino dei dati in caso di minaccia informatica. In base a una ricerca di Forrester Consulting, in caso di attacco informatico, PowerProtect Cyber Recovery aiuta a ridurre il downtime del 75% e aiuta a ridurre dell'80% le ore dedicate al ripristino.[3]

PowerProtect Cyber Recovery offre la sicurezza necessaria per identificare e ripristinare rapidamente dati ottimi noti e riprendere le normali operazioni di business dopo un attacco informatico. È il momento di tornare al business.

[1] Dati basati sulla ricerca di Vanson Bourne commissionata da Dell Technologies, "Global Data Protection Index 2024 Snapshot". Ottobre 2023.
[2] Dati basati sul report ESG commissionato da Index Engines, "Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption". Giugno 2024
[3] Ricerca di Forrester Consulting commissionata da Dell Technologies, "The Total Economic Impact of Dell PowerProtect Cyber Recovery", agosto 2023



Ulteriori informazioni su Dell PowerProtect Cyber Recovery

Contatta un esperto Dell Technologies

Visualizza altre risorse

Partecipa alla conversazione con #PowerProtect

DELL Technologies