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 distruggere, rubare o in qualche modo 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. L'azienda sarebbe in grado di sopravvivere? Ecco i componenti di una soluzione cyber-resiliente:

Isolamento e governance dei dati
Un ambiente di data center isolato, scollegato dalle reti aziendali e di backup e con limitazioni di accesso per utenti diversi da quelli con autorizzazione adeguata.

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 e strumenti intelligenti
Apprendimento automatico e indicizzazione completa dei contenuti sulla base di analisi efficaci, con tutta la sicurezza del vault, oltre a controlli automatizzati dell'integrità volti a individuare i dati interessati da malware e strumenti per l'eventuale correzione.

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 delle soluzioni
Istruzioni di esperti per la selezione di data set, applicazioni e altri asset critici al fine di stabilire gli obiettivi RTO/RPO e semplificare il ripristino.

Attacchi informatici: il nemico delle aziende con un approccio basato sui dati

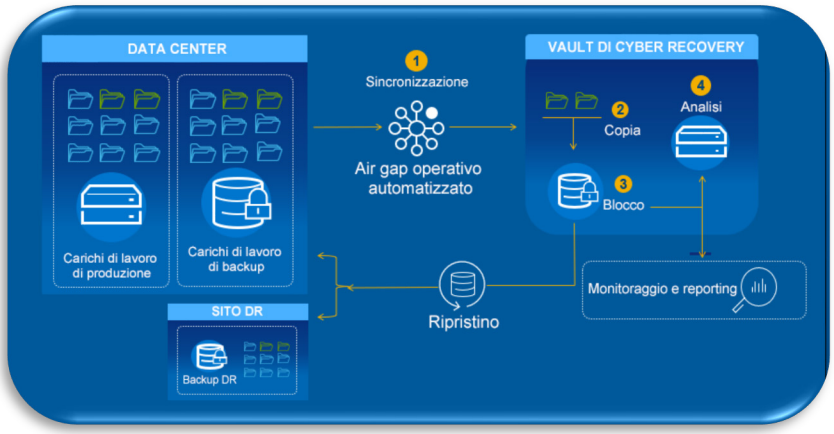
I dati sono la "valuta" dell'Internet Economy, nonché asset critici da proteggere e rendere disponibili in tempi rapidissimi, garantendone al contempo la riservatezza. Il mercato globale di oggi è caratterizzato dal flusso costante di dati su reti interconnesse e le iniziative di Digital Transformation mettono a rischio i dati più 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].

Cosa fare quindi per proteggere l'organizzazione, i clienti, i dipendenti e i dati più importanti?

La soluzione: Dell PowerProtect Cyber Recovery



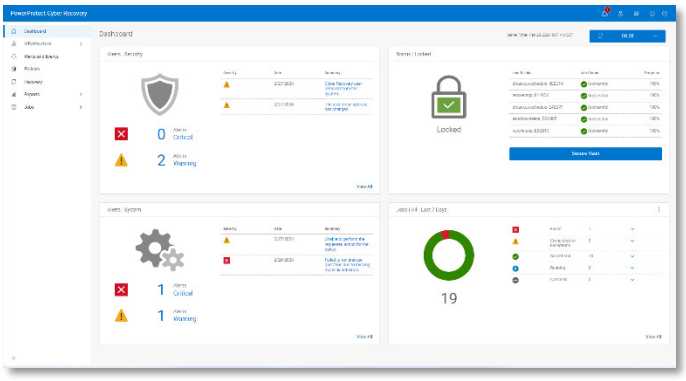
Per ridurre i rischi per il business associati agli attacchi informatici e creare un approccio più cyber-resiliente alla protezione dei dati, è possibile modernizzare e automatizzare le strategie di ripristino e continuità aziendale, oltre a sfruttare gli strumenti intelligenti più recenti per rilevare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

PowerProtect Cyber Recovery: immutabilità, isolamento e intelligenza

Vault di Cyber Recovery

Il vault di PowerProtect Cyber Recovery offre diversi livelli di protezione per fornire resilienza contro gli attacchi informatici, anche in caso di minaccia interna. Questo sistema, che richiede credenziali di sicurezza separate e l'autenticazione a più fattori per l'accesso, allontana i dati critici dalla superficie di attacco, isolandoli fisicamente in una zona protetta del data center. Tra le protezioni aggiuntive figura un air gap operativo automatizzato per garantire l'isolamento della rete ed eliminare interfacce di gestione che sono possibili obiettivi di compromissione. PowerProtect Cyber Recovery automatizza la sincronizzazione dei dati tra i sistemi di produzione, inclusi open system e mainframe, e il vault, creando copie non modificabili con policy di retention bloccate. In caso di attacco informatico è possibile identificare rapidamente una copia pulita dei dati, ripristinare i sistemi critici e riprendere le normali operazioni di business.



CyberSense

PowerProtect Cyber Recovery è la prima soluzione per l'integrazione completa di CyberSense, che aggiunge un livello di protezione intelligente per agevolare la ricerca dei dati danneggiati nel caso in cui l'attacco arrivasse al data center. Questo approccio innovativo offre funzionalità di indicizzazione completa dei contenuti e utilizza l'apprendimento automatico basato sull'AI per analizzare più di 200 statistiche basate sui contenuti e rilevare eventuali segni di danneggiamento dovuti a ransomware. CyberSense rileva i dati danneggiati con un'attendibilità fino al 99,5%, aiutando le aziende a identificare le minacce, diagnosticare i vettori di attacco e proteggere i contenuti business-critical, il tutto con la sicurezza del vault.

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 anche report forensi post-attacco per comprendere la profondità e l'ampiezza dell'attacco 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. Automatizza la creazione dei punti di ripristino utilizzati per il ripristino o l'analisi della sicurezza.

Pianificazione e progettazione delle soluzioni

Grazie ai servizi di consulenza Dell opzionali è possibile stabilire quali sistemi business-critical proteggere e creare mappe di dipendenza 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.

Per proteggere i dati essenziali dagli attacchi informatici, sono necessarie soluzioni collaudate, moderne e resilienti. 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.

[1] Dati basati sulla ricerca di Vanson Bourne commissionata da Dell Technologies, "Global Data Protection Index 2023 Snapshot", ottobre 2023.

Ulteriori informazioni su Dell PowerProtect Cyber Recovery	Contatta un esperto Dell Technologies	Visualizza altre risorse	Partecipa alla conversazione con #PowerProtect