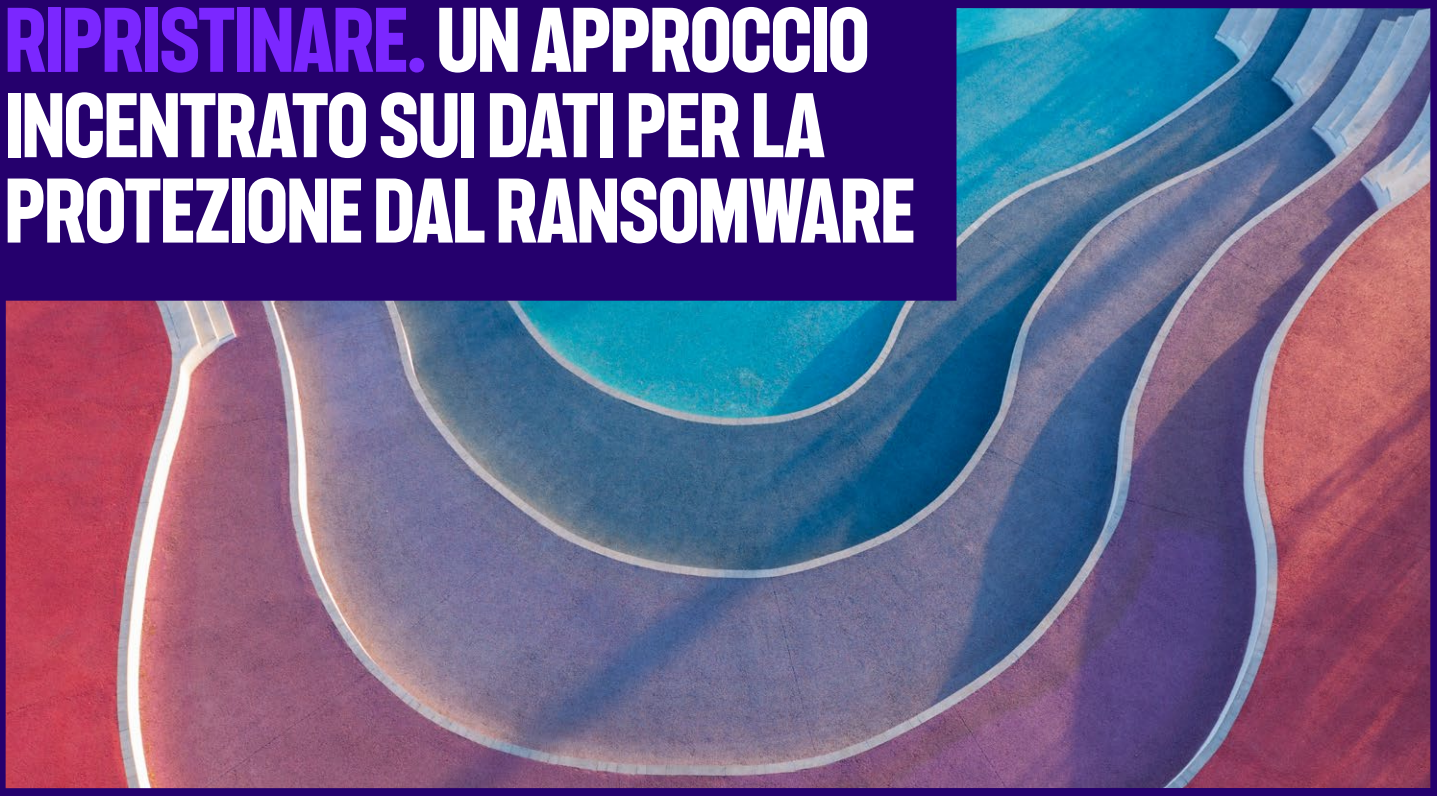
NetApp

PROTEGGERE. RILEVARE. RIPRISTINARE. UN APPROCCIO INCENTRATO SUI DATI PER LA PROTEZIONE DAL RANSOMWARE



Proteggere: Metti al sicuro il tuo ambiente.
Rilevare: Anticipa le minacce.
Ripristinare: Recupera rapidamente.

La sfida
Gli attacchi ransomware sono una minaccia sempre più diffusa e sofisticata per le organizzazioni di ogni dimensione. Questi attacchi dannosi crittografano preziosi dati e richiedono il pagamento per il loro rilascio, spesso causando significative perdite finanziarie e interruzioni operative.

- Gli incidenti informatici sono il principale rischio aziendale a livello globale.
- Si prevede che il ransomware colpisca ogni 2 secondi entro il 2031.
- l'anno scorso, il 59% delle organizzazioni è stato colpito da ransomware.
- Gli attacchi ransomware sono aumentati del 73% dal 2022 al 2023.

Sebbene molte aziende si concentrino sulla sicurezza di reti e endpoint, è cruciale non trascurare l'importanza della protezione del layer di storage in cui risiedono i dati. Implementando efficaci misure di sicurezza a livello di storage, come crittografia, controlli di accesso e backup immutabili, puoi creare una linea aggiuntiva di difesa contro i ransomware.

Questo approccio aiuta a proteggere i dati alla loro origine, rendendo più difficile per gli autori degli attacchi crittografare o corrompere le informazioni critiche. Le soluzioni di storage sicuro possono contribuire a tempi di recovery più rapidi e ridurre al minimo la perdita di dati in caso di attacco di successo, sottolineando l'importanza di una strategia di sicurezza completa che include il rafforzamento dell'infrastruttura storage.

Resilienza informatica di NetApp: Un approccio alla protezione dal ransomware incentrato sui dati

La protezione contro gli incidenti informatici comprende più livelli di difesa per la protezione contro un'ampia gamma di minacce. Una forte difesa informatica inizia dal livello di **sicurezza dell'identità** che, insieme al livello più esterno, **la sicurezza perimetrale** , agisce come la prima linea di difesa.

La sicurezza della rete si basa su questa base per proteggere i dati in transito e rilevare le attività anomale all'interno della rete interna. **La sicurezza degli endpoint** aggiunge un livello di difesa per i singoli dispositivi connessi alla rete. **La sicurezza delle applicazioni** si concentra sulla protezione delle applicazioni software da vulnerabilità e attacchi.

Infine, il fulcro della posizione di sicurezza risiede nella **sicurezza dei dati**, che salvaguarda la risorsa più preziosa di un'organizzazione: I dati e le risorse più mission-critical. Questo livello generalmente include la protezione dei dati con solide soluzioni di backup e ripristino.

Insieme, questi livelli di sicurezza interconnessi creano una strategia di difesa completa progettata per proteggere le risorse digitali dell'azienda dal perimetro al data center, affrontando le minacce a ogni livello dell'infrastruttura IT.

La protezione nel layer di dati delle risorse mission-critical è ancora più importante e ha requisiti unici. Per essere efficaci, le soluzioni di questo livello devono offrire questi quattro attributi critici:

- Protezione in base alla progettazione per ridurre al minimo le possibilità di un attacco di successo contro la tua organizzazione
- Rilevamento e risposta in tempo reale per ridurre al minimo l'impatto di un attacco riuscito
- Protezione WORM (Write Once, Read Many) a mappatura aerea per isolare i backup dei dati critici
- Un pannello di controllo semplice per una protezione completa dal ransomware e un recovery rapido

NetApp è in grado di rilevare, proteggere ed eseguire il ripristino nel layer di dati.

Sicuro per design: Protezione ransomware integrata ONTAP nativa nello storage
Il software NetApp ONTAP offre un'efficace protezione dal ransomware tramite un approccio sicuro per progettazione. Le funzionalità di base del prodotto includono copie Snapshot immutabili e non cancellabili, in modo che i dati rimangano inalterabili e non possano essere eliminati, anche dagli amministratori, creando un punto di fallback affidabile per il recovery. La funzionalità ONTAP FPolicy migliora la sicurezza bloccando i file dannosi, impedendo la diffusione di minacce all'interno del sistema.

BENEFICI PRINCIPALI

- **Sicuro fin dalla progettazione** Data Protection integrata al layer di storage.
- **Rilevamento e risposta in tempo reale.** Difesa ransomware ai-powered.
- **Cyber vaulting.** Backup immutabili e indelebili.
- **Control plane unificato.** Orchestrazione intelligente, dal rilevamento al recovery.
- **Garanzia di recovery.** Nessuna perdita di dati con le copie Snapshot di NetApp.

Per rafforzare i controlli degli accessi, la verifica multiamministratore richiede a più amministratori l'approvazione di azioni critiche, riducendo il rischio di minacce interne o credenziali compromesse. Inoltre, l'autenticazione multifattore aggiunge un ulteriore livello di sicurezza, il che significa che solo il personale autorizzato può accedere a dati e sistemi sensibili.

Rilevamento e risposta in tempo reale
In aggiunta alla nostra efficace protezione dal ransomware, NetApp offre un rilevamento in real-time con precisione del 99% e funzionalità di risposta near-Instant, sfruttando la tecnologia autonoma basata su ai integrata direttamente in ONTAP. Questo rilevamento avanzato monitora costantemente l'eventuale presenza di attività e anomalie sospette, identificando rapidamente i potenziali attacchi ransomware man mano che si diffondono nel cloud di file, blocchi e nativi in Amazon FSX per ONTAP. Quando viene rilevata una minaccia, il sistema può isolare automaticamente i dati interessati e impedire un'ulteriore diffusione, riducendo al minimo i potenziali danni.

Le informazioni sull'infrastruttura dati di NetApp (DII) offrono un livello supplementare di difesa contro le minacce interne. Rileva il potenziale comportamento anomalo degli utenti e intraprende azioni immediate come bloccare l'accesso degli utenti ai sistemi storage e acquisire snapshot. Inoltre, DII fornisce analisi dettagliate per l'analisi forense e l'auditing. Questo approccio completo combina il rilevamento proattivo delle minacce, meccanismi di risposta rapida e il monitoraggio dettagliato delle attività degli utenti, offrendo uno scudo dalle molte sfaccettature contro gli attacchi ransomware esterni e le minacce interne.

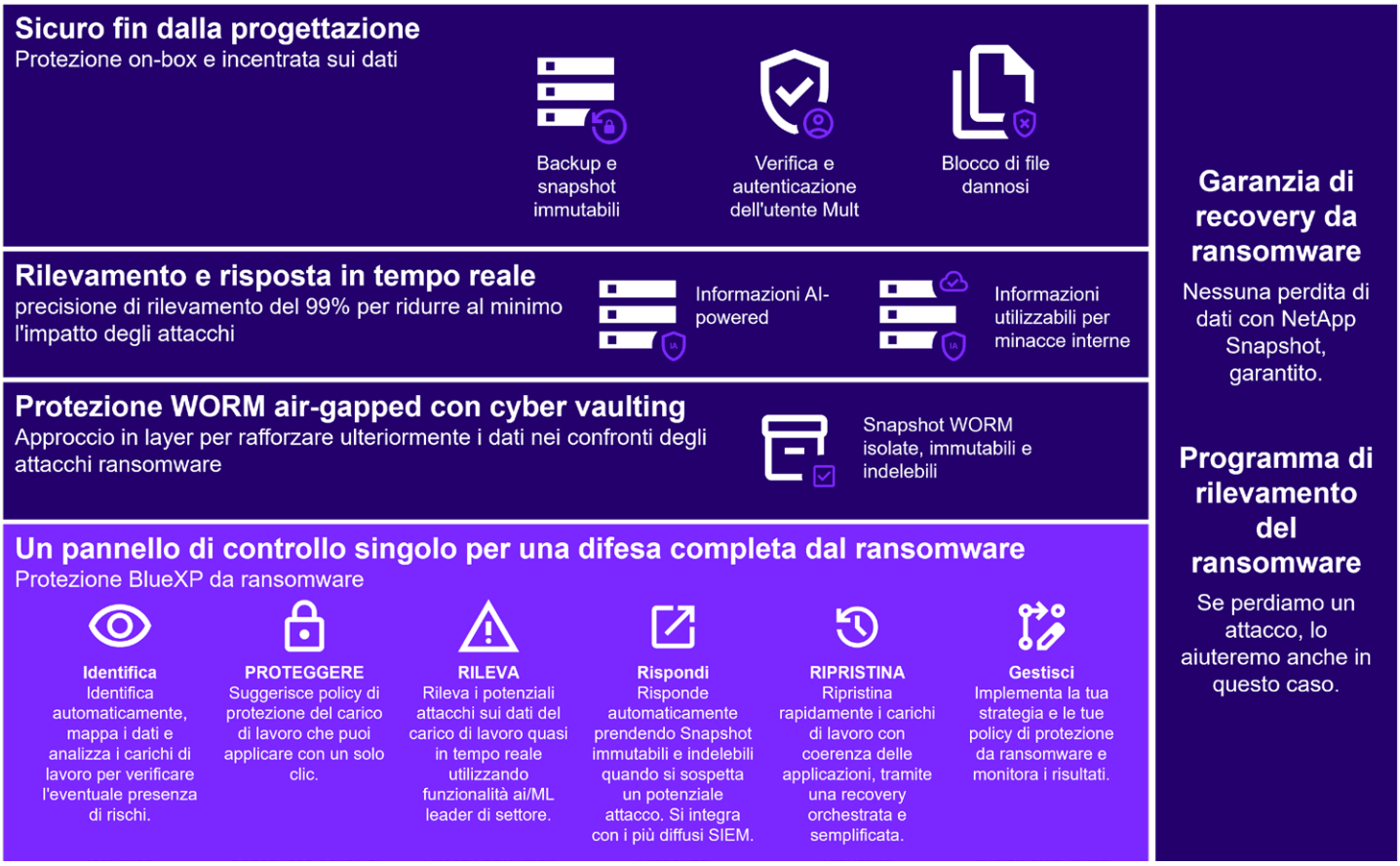


Figura 1: NetApp offre lo storage dei dati più sicuro al mondo, con difese multilivello per proteggere i dati in modo intelligente ed efficiente, incluso l'accesso ai dati tramite crittografia end-to-end, autenticazione multifattore e accesso in base al ruolo.

Backup isolati per il cyber vaulting
NetApp cybervaulting, basato sul software di conformità SnapLock®, offre alle organizzazioni una soluzione completa e flessibile per proteggere le loro risorse di dati più critiche. L'air-gapping logico con solide metodologie di indurimento per ONTAP ti consente di creare ambienti storage isolati e sicuri, resilienti rispetto a minacce informatiche in evoluzione. Con NetApp, puoi avere fiducia nella riservatezza, nell'integrità e nella disponibilità dei tuoi dati, mantenendo al contempo l'agilità e l'efficienza della tua infrastruttura storage.

Per una maggiore sicurezza, NetApp ti consente di creare un livello aggiuntivo di data Protection:

- Infrastruttura di storage sicura e isolata (ad esempio, sistemi di storage air-gapped)
- Copie di backup dei tuoi dati immutabili e indelebili
- Rigidi controlli degli accessi e autenticazione multifattore
- Funzionalità di ripristino rapido dei dati
- Applicando LA tecnologia WORM, SnapLock impedisce la crittografia e l'eliminazione dei dati mediante copie dei dati indistruttibili ed efficienti

Piano di controllo semplice e robusto
NetApp è l'unico fornitore di storage che offre un unico piano di controllo con NetApp BlueXP™ per coordinare ed eseguire in modo intelligente le tecnologie di difesa anti-ransomware end-to-end incentrate sul carico di lavoro. Con queste tecnologie, potrai **identificare e proteggere** i dati critici dei workload a rischio con un singolo clic; **rilevare e rispondere in** modo accurato e automatico per limitare l'impatto di potenziali attacchi e **ripristinare i** carichi di lavoro entro pochi minuti, e non giorni o mesi, proteggendo i tuoi preziosi dati dei carichi di lavoro e riducendo al minimo il costo dell'interruzione del business.

BlueXP ransomware Protection orchestrator unisce le potenti funzionalità di NetApp ONTAP con i servizi dati BlueXP, aggiungendo intelligenza artificiale e consigli basati su machine learning con workflow automatizzati per aiutarti a:

- **Identificare.** Identifica automaticamente i carichi di lavoro e i relativi dati nello storage NetApp, associa i dati al carico di lavoro e determina la sensibilità, l'importanza e il rischio dei dati dei carichi di lavoro.
- **Proteggere.** Suggerisce policy di protezione del carico di lavoro che puoi applicare con un solo clic.

- **Rilevare.** Rileva i potenziali attacchi ai dati del tuo carico di lavoro con rilevamento basato su ML leader del settore che opera quasi in tempo reale.
- **Rispondere.** Rispondere automaticamente quasi in tempo reale creando copie Snapshot immutabili quando si sospetta un potenziale attacco.
- **Ripristinare.** Identificare il miglior recovery point e ripristinare rapidamente i carichi di lavoro e i dati associati tramite una recovery orchestrata semplificata.

"Abbiamo assistito di recente a un evento ransomware e quando abbiamo visto cosa offre il rilevamento dei ransomware di Cloud Insights, siamo rimasti colpiti."

Director dell'IT, Transportation Company

BlueXP ransomware Protection orchestrator rimuove l'onere e l'ansia di difendere i carichi di lavoro dai downtime correlati al ransomware e dalla perdita di dati, mettendo a disposizione una soluzione completa che ti assisterà nella preparazione al ransomware, risponderà agli attacchi e ti guiderà attraverso il recovery. Solo NetApp garantisce che quando si verifica un attacco, lo saprai immediatamente, verranno protetti i dati importanti dei tuoi carichi di lavoro e il recovery sarà più semplice e rapido, in modo da ridurre al minimo le interruzioni del business.

La protezione dal ransomware di NetApp ti aiuta a identificare e proteggere i dati dove risiedono, rilevare e rispondere in modo accurato e automatico per limitare l'impatto dei potenziali attacchi e ripristinare i dati entro pochi minuti, e non giorni o mesi. Questa funzionalità aiuta a preservare i tuoi dati preziosi e a ridurre al minimo le costose interruzioni della resilienza informatica.

Il ransomware può debilitare le aziende che non lo prendono sul serio. Solo l'approccio di resilienza informatica incentrato sui dati di NetApp offre sicurezza e protezione complete e integrate per i dati primari e secondari con una garanzia di aiuto per il ripristino.

Ulteriori informazioni sulle soluzioni NetApp contro il ransomware

Contattaci

A proposito di NetApp

NetApp è l'azienda di infrastrutture dati intelligenti che combina storage unificato, servizi dati integrati e soluzioni CloudOps, per trasformare i vincoli in opportunità, per ogni cliente. NetApp crea infrastrutture indipendenti da silos e, sfruttando l'Intelligenza Artificiale, abilita la miglior gestione dei dati del settore. Il nostro storage, l'unico servizio enterprise integrato nativamente nelle principali soluzioni cloud del mondo, offre una flessibilità perfetta. Inoltre, i nostri servizi dati consentono di ottenere un vantaggio competitivo grazie a una governance, una resilienza informatica e un'agilità delle applicazioni di livello superiore. Le nostre soluzioni CloudOps forniscono ottimizzazione continua delle performance ed efficienza attraverso l'Intelligenza Artificiale. A prescindere dal tipo di dati, dal carico di lavoro o dall'ambiente, con NetApp puoi trasformare la tua infrastruttura dati per aumentare le opportunità di business.
www.netapp.com

NetApp