Resilienza dei dati Zero Trust (ZTDR)

Architettura di backup e ripristino dei dati sicura
Un approccio pragmatico all'implementazione di Zero Trust

Panoramica

Le organizzazioni di tutte le dimensioni e di tutti i settori comprendono l'importanza di Zero Trust per garantire la sicurezza dei propri dati e della propria attività. Tuttavia, l'attuale modello Zero Trust deve ancora essere applicato in modo significativo al backup e al ripristino dei dati. Il concetto di estensione dei principi Zero Trust al backup e al ripristino dei dati è in linea con la natura olistica della cybersecurity e la protezione delle informazioni sensibili non si limita alla sicurezza perimetrale.

Per affrontare questa sfida, Veeam ha collaborato con l'esperto di Zero Trust, Jason Garbis di Numberline Security, sul framework di resilienza dei dati Zero Trust, progettato per ridurre al minimo i rischi, rafforzare la protezione dei dati e rivoluzionare il livello di sicurezza di un'organizzazione. Questo framework si basa sul modello di maturità Zero Trust (ZTMM) della Cybersecurity and Infrastructure security Agency (CISA) ed estende i principi fondamentali di ZTMM a uno scenario di backup e ripristino. Il framework di resilienza dei dati Zero Trust implica che la fiducia non sia mai data per scontata e che le misure di sicurezza siano applicate in modo coerente durante l'intero ciclo di vita dei dati, compreso il processo di backup e ripristino; si tratta di un modello pratico che aiuterà sia i team IT che quelli della sicurezza a ridurre significativamente i rischi, migliorare la protezione dei dati e aumentare notevolmente il livello di sicurezza di qualsiasi organizzazione.

Vuoi saperne di più sulla resilienza dei dati Zero Trust? Scarica subito il white paper

L'approccio di Veeam a Zero Trust: Resilienza dei dati Zero Trust (ZTDR)

Zero Trust è fondamentale per la strategia di sicurezza di un'organizzazione e i principi chiave come la segmentazione tra le risorse di dati più critiche, l'accesso con privilegi minimi e l'autenticazione e l'autorizzazione continue con le best practice di Identity and Access Management (IAM) sono particolarmente rilevanti quando si tratta di salvaguardare gli ambienti di backup. Incorporando una funzione di resilienza dei dati Zero Trust, le organizzazioni possono affrontare le sfide specifiche poste dalle soluzioni di protezione dei dati e garantire una strategia di sicurezza completa per le organizzazioni, indipendentemente dal fatto che si trovino on-premises, nel cloud o in ambienti ibridi.

Un concetto fondamentale di Zero Trust è quello di presupporre sempre una violazione, indipendentemente dalla sicurezza di un determinato ambiente. Nella metodologia ZTDR, una tecnica fondamentale per combattere questo rischio è la separazione del software di gestione del backup e dello storage di backup in zone di resilienza o domini di sicurezza separati, isolando i dati di backup da eventuali minacce al software di gestione del backup, siano esse interne o esterne. Veeam supporta diverse tecnologie per creare zone di resilienza con uno storage immutabile e altamente sicuro (vedi Figura 1).

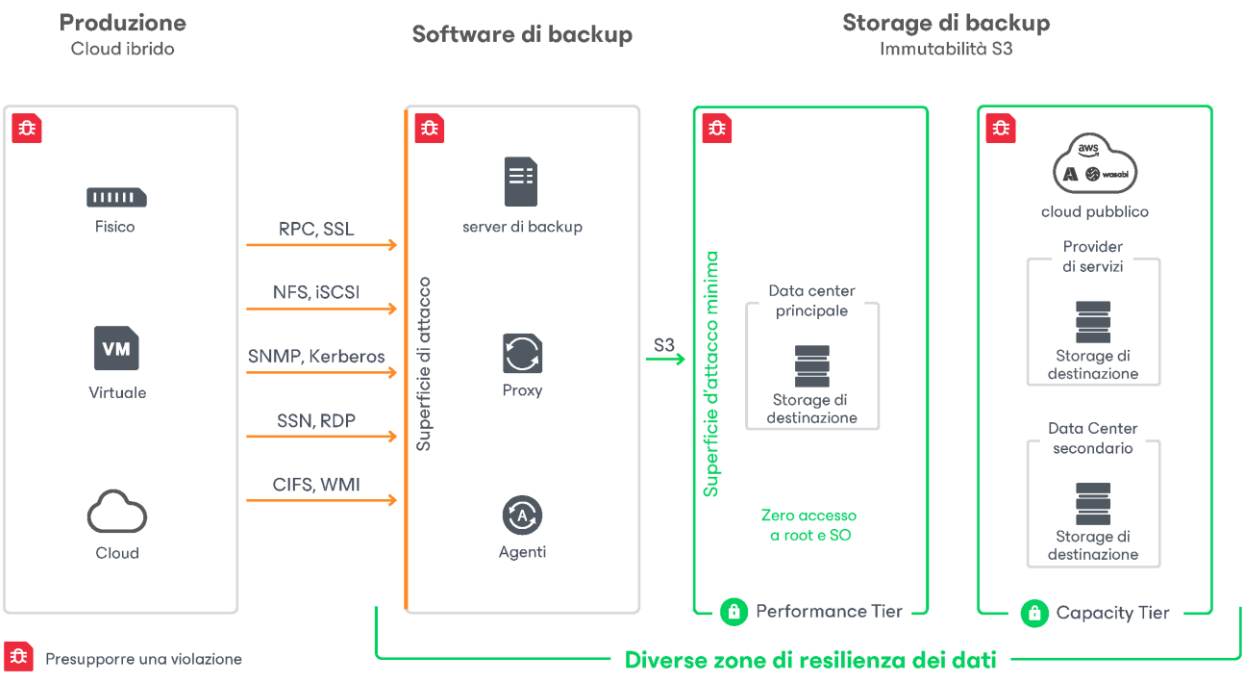

Figura 1

Poiché le soluzioni di protezione dei dati presentano alcuni dei più alti livelli di accesso in lettura e scrittura ai dati di produzione in tutta l'organizzazione, e spesso ai dati più critici, è fondamentale che l'ambiente di backup di un'organizzazione sia sicuro e protetto tramite le best practice Zero Trust.

Principi di resilienza dei dati Zero Trust

Sulla base del modello di maturità Zero Trust della CISA (vedi Figura 2), ci sono considerazioni aggiuntive che un'organizzazione dovrebbe applicare specificamente al pilastro dei dati.

Modello di maturità Zero Trust della CISA

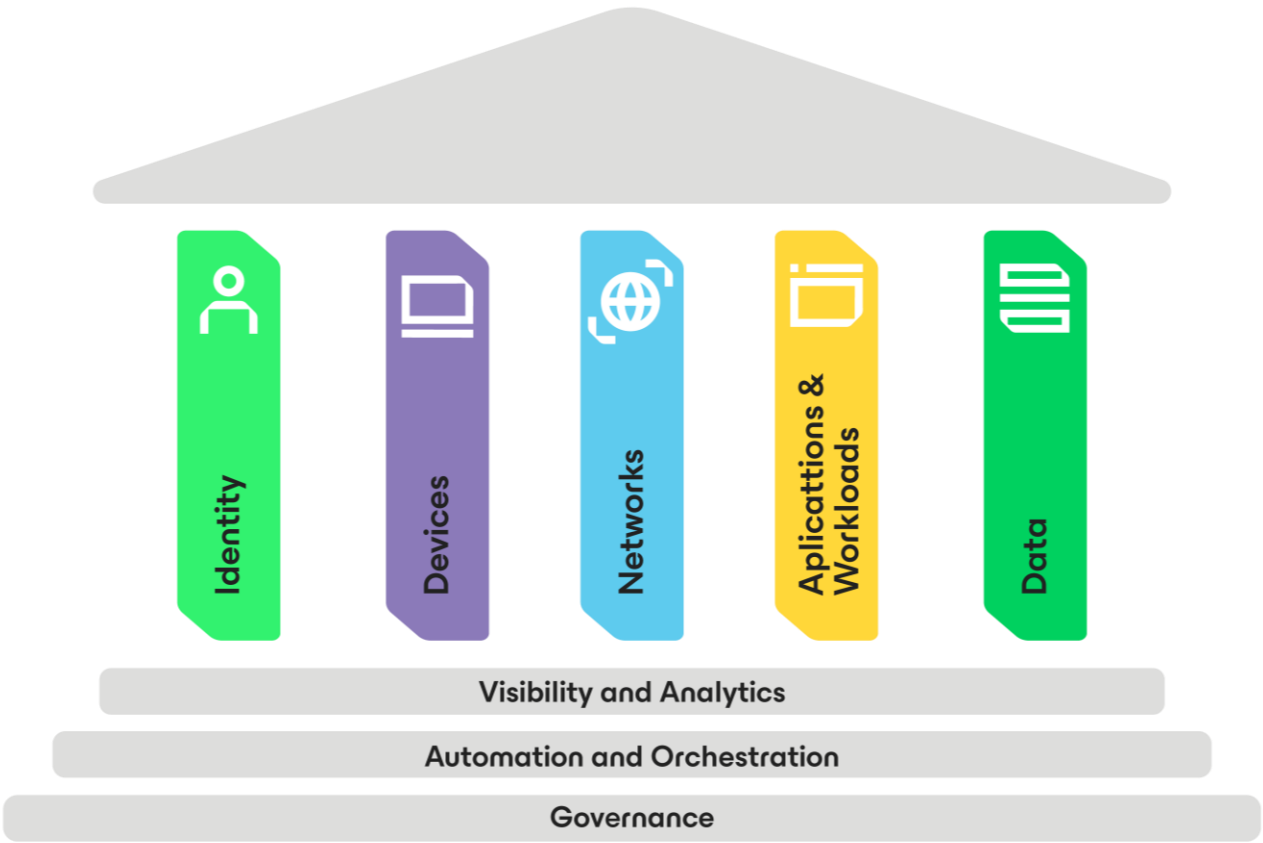

Figura 2

L'articolo di ricerca sulla resilienza dei dati Zero Trust evidenzia 5 principi fondamentali della resilienza dei dati Zero Trust (ZTDR) per contribuire alla strategia complessiva di resilienza informatica dell'organizzazione, garantendo la protezione delle risorse di dati critici di fronte all'evoluzione delle minacce informatiche.

Accesso con privilegio minimo

Questo principio enfatizza la concessione dell'accesso a una persona, un processo, un dispositivo o un carico di lavoro essenziale per svolgere la funzione prevista.

Accesso controllato per l'infrastruttura di backup:

- L'implementazione di policy Zero Trust per il controllo dell'accesso all'infrastruttura di backup garantisce che solo gli utenti convalidati possano stabilire connessioni alla soluzione di backup. Si tratta di un passaggio fondamentale per prevenire l'accesso non autorizzato e le potenziali violazioni dei dati.

Ruoli self-service granulari e ruoli di amministratore del backup con restrizioni:

- L'offerta di ruoli self-service granulari e di ruoli di amministratore del backup limitati all'interno di Veeam dimostra l'impegno verso il principio del privilegio minimo. Ciò garantisce che gli utenti abbiano accesso solo alle funzioni specifiche necessarie per le loro attività, riducendo la probabilità di un uso improprio involontario o intenzionale.

Best practice per l'Identity and Access Management (IAM):

- L'applicazione delle best practice IAM, come l'utilizzo dell'autenticazione a più fattori (MFA), aggiunge un ulteriore livello di sicurezza all'ambiente di backup. Si tratta di una misura fondamentale per impedire l'accesso non autorizzato, specialmente alla luce degli elevati livelli di privilegi associati alle soluzioni di backup.

Principio dei "quattro occhi" per decisioni operative critiche:

- L'integrazione del principio dei "quattro occhi" per le decisioni operative critiche garantisce che le azioni chiave richiedano l'approvazione o la verifica di almeno due persone autorizzate. Questo aggiunge un ulteriore livello di supervisione e riduce il rischio di attività dannose o errate.

Immutabilità

Anche con un perimetro di rete sicuro, un concetto critico di Zero Trust è quello di presupporre una compromissione. L'immutabilità dei backup è un potente meccanismo di difesa, in quanto garantisce che un criminale interno o esterno non possa modificare o eliminare i dati di backup critici.

Segmentazione per ridurre al minimo la superficie d'attacco e l'area di impatto:

- Segmentare il software di backup e lo storage di backup in zone di resilienza separate è il concetto chiave di ZTDR. In questo modo si riduce al minimo il potenziale impatto di minacce interne o esterne isolando i componenti critici. Garantire che il software di backup non disponga di autorizzazioni a livello di sistema operativo/gestione per lo storage di backup aggiunge un ulteriore livello di protezione.

Zone di resilienza multiple e 3-2-1-1 regola del backup:

- Più zone di resilienza dei dati o domini di sicurezza forniscono una sicurezza a più livelli. Inoltre, la regola del backup 3-2-1-1 è una best practice per la strategia di backup e si allinea bene con i principi di resilienza dei dati. Avere almeno tre copie di dati, su due diversi tipi di supporto, e con almeno una copia off-site e almeno una fisicamente isolata o immutabile fornisce una sicurezza a più livelli, riducendo il rischio di perdita di dati.

Zone di resilienza

Un concetto fondamentale di Zero Trust per il networking è la microsegmentazione per suddividere i perimetri di sicurezza in zone più piccole, riducendo così la superficie di attacco, il raggio di esplosione di qualsiasi zona compromessa e il movimento laterale di un aggressore. Per ZTDR, questo concetto può essere applicato utilizzando le zone di resilienza dei dati. Le zone di resilienza separano lo storage di backup e isolano il piano di controllo dello storage dal software di backup e dal relativo piano di controllo. Ciò fornisce una linea di demarcazione critica che garantisce la sopravvivenza dei dati di backup anche in caso di software di backup compromesso. Ciò può accadere per numerosi motivi, comprese le minacce interne. Un sistema di backup deve garantire che i dati di backup possano essere ripristinati in modo semplice e veloce da un'installazione pulita del software di backup.

Infrastruttura di produzione

Infrastruttura Veeam

Dati di backup autonomi

Backup | Crittografato | 3-2-1-1-0

Integrità dei dati e sicurezza migliorata:

- La configurazione di un repository di backup compatibile e l'impostazione di un periodo di retention per i backup immutabili è una misura proattiva per garantire l'integrità dei dati e una maggiore sicurezza. I backup immutabili fungono da protezione dagli attacchi ransomware e da altre forme di manipolazione dei dati.

Resilienza del sistema

Un approccio olistico alla sicurezza IT comprende la resilienza di tutto l'ecosistema, comprese piattaforme, strumenti, tecnologie e processi. Le diverse opzioni di resilienza di Veeam dimostrano l'impegno a fornire alle organizzazioni gli strumenti per resistere a vari tipi di interruzioni, inclusa una perdita completa del sistema.

Rilevamento dello scostamento temporale per backup immutabili:

- L'implementazione del rilevamento dello scostamento temporale è una misura proattiva per prevenire l'eliminazione di backup immutabili, anche a fronte di NTP (Network Time Protocol) compromessi. Questa funzionalità migliora la sicurezza e l'affidabilità dei repository di backup, garantendo l'integrità dei dati di backup critici.

Opzioni di ripristino flessibili:

- Veeam offre opzioni di ripristino flessibili, anche in ambienti diversi, e supporta implementazioni fisiche e virtuali, nonché ambienti ibridi, per allinearsi con le diverse infrastrutture IT gestite dalle organizzazioni. Questa flessibilità consente alle organizzazioni un ripristino veloce: ad esempio da VMware on-premises ad AWS o Azure oppure da AWS ad Azure nel caso in cui l'ambiente originale non sia disponibile.

Opzioni di ripristino granulare dei dati:

- La flessibilità nel ripristino dei dati in diversi ambienti e con diverse granularità migliora la resilienza complessiva dei dati. Questa adattabilità consente alle organizzazioni di personalizzare i processi di ripristino in base alle esigenze specifiche dei diversi scenari.

Convalida proattiva

La costante convalida degli aspetti funzionali e dei processi è fondamentale per garantire che i dati rimangano protetti e che eventuali anomalie vengano rilevate e risolte tempestivamente.

Monitoraggio e convalida continui:

- L'enfasi sui sistemi di monitoraggio 365/24/7 riflette la consapevolezza che le minacce alla sicurezza informatica possono emergere in qualsiasi momento. Avendo a disposizione informazioni in tempo reale sullo stato dell'ambiente, gli amministratori possono rilevare tempestivamente eventuali anomalie, consentendo alle organizzazioni di indagare e rispondere prima che si verifichi un potenziale attacco informatico o perdita di dati.

- Sfruttare strumenti come Veeam ONE per il monitoraggio rappresenta un approccio proattivo al mantenimento dell'integrità e della sicurezza degli ambienti di backup e ripristino. La capacità di Veeam ONE di monitorare diversi parametri, tra cui l'utilizzo della CPU, la velocità di scrittura del datastore, la velocità di trasmissione di rete e le dimensioni del backup incrementale, fornisce alle organizzazioni preziose informazioni su potenziali problemi.

Visibilità completa

- Il concetto di visibilità completa in tutta l'infrastruttura di protezione dei dati è essenziale. Garantisce che le organizzazioni abbiano una comprensione completa dello stato di salute e dello stato dei propri sistemi di backup e ripristino, consentendo loro di prendere decisioni informate e agire rapidamente quando necessario.
- Come parte integrante della recente release 12.1 di Veeam, il nuovo Centro minacce Veeam aggrega le informazioni provenienti dall'intera piattaforma e dall'infrastruttura, combinandole in un unico pannello di gestione che evidenzia le minacce, identifica i rischi e fornisce alle organizzazioni una scheda di valutazione per la sicurezza semplice e potente per l'intero ambiente di protezione dei dati.

Semplicità operativa

L'importanza della semplicità operativa durante i disastri o gli eventi di sicurezza informatica è il riconoscimento del ruolo fondamentale svolto dalla semplicità in un ripristino efficace. Più lunga è la durata delle interruzioni, maggiore è l'impatto sulle operazioni e sui profitti di un'organizzazione.

Tempo di un'interruzione medio in caso di attacchi ransomware:

- Come riportato nel Report sulle tendenze nel ransomware 2023 di Veeam, il tempo medio di interruzione dovuto a un attacco ransomware è di tre settimane. Ciò sottolinea l'urgenza e l'importanza di un rapido ripristino, particolarmente importante durante le situazioni di alta pressione in cui ogni momento può fare la differenza.

Bilanciamento di strumenti, persone e processi:

- Trovare il giusto equilibrio tra strumenti, persone e processi è una sfida fondamentale, in particolare quando le organizzazioni devono affrontare un disastro o un attacco informatico. La semplicità operativa implica la semplificazione dei flussi di lavoro, l'ottimizzazione dei processi e la garanzia che siano disponibili gli strumenti giusti per un ripristino efficiente.

Investimento nella semplificazione delle capacità di ripristino:

- I leader di settore come Veeam investono in modo proattivo per fornire capacità di ripristino gestendone le complessità. La possibilità di ripristinare i dati da una piattaforma all'altra e di sfruttare strumenti come l'orchestrator del ripristino di Veeam dimostra la dedizione alla semplificazione di scenari di ripristino complessi e mantiene i piani di failover aggiornati, automatizzati e completamente testati, garantendo la preparazione durante gli scenari di alta pressione.

Scopri le ultime funzionalità di sicurezza nella versione 12.1

Conclusione

Man mano che il nostro panorama digitale si evolve e si espande, lo fanno anche gli attacchi informatici e le capacità degli attori delle minacce. Di conseguenza, abbiamo un urgente bisogno di unificare e rafforzare la collaborazione e l'efficacia dell'IT e della sicurezza per proteggere e difendere meglio i dati, i dispositivi e le persone delle nostre organizzazioni. Questo viaggio verso la maturità non avverrà da un giorno all'altro, ma è imperativo che questo inizi ad accadere il prima possibile. Il primo passo è Zero Trust. Il modello di maturità Zero Trust (ZTMM) della CISA fornisce i principi fondamentali per la sicurezza e la protezione di un'organizzazione, ma non copre tutto. L'introduzione di Zero Trust Data Resilience (ZTDR) come estensione dello Zero Trust Maturity Model (ZTMM) della CISA è un approccio strategico e lungimirante per affrontare il panorama in evoluzione delle minacce informatiche.

L'integrazione dei principi ZTDR, tra cui l'accesso con privilegi minimi, l'immutabilità, la resilienza del sistema, la convalida proattiva e la semplicità operativa, dimostra una strategia completa per la sicurezza e la protezione dei dati aziendali. Adottando la ZTDR, le organizzazioni avranno un percorso chiaro e concreto per rafforzare la loro postura di sicurezza. Ciò significa operazioni più efficienti e allineamento tra i team IT e di sicurezza che, in ultima analisi, condurrà a un ripristino più rapido e sicuro.

Informazioni su Veeam Software

Veeam, leader globale di mercato in protezione dei dati e ripristino dal ransomware ha la missione di aiutare ogni organizzazione non solo a riprendersi da un'interruzione o da una perdita di dati, ma ad andare oltre. Con Veeam, le organizzazioni raggiungono una resilienza radicale attraverso la sicurezza, il ripristino e la libertà dei dati per il cloud ibrido. La Veeam Data Platform offre un'unica soluzione per ambienti cloud, virtuali, fisici, SaaS e Kubernetes, offrendo ai responsabili IT e della sicurezza la tranquillità che dati e applicazioni sono protetti e sempre disponibili. Con sede a Columbus, Ohio, e uffici dislocati in oltre 30 Paesi, Veeam protegge più di 450.000 clienti in tutto il mondo, tra cui il 73% delle aziende Global 2000, che si affidano a Veeam per mantenere in funzione le loro attività. La resilienza radicale inizia con Veeam. Per maggiori informazioni, visita www.veeam.com/it o segui Veeam su LinkedIn @veeam-software e X @veeam.