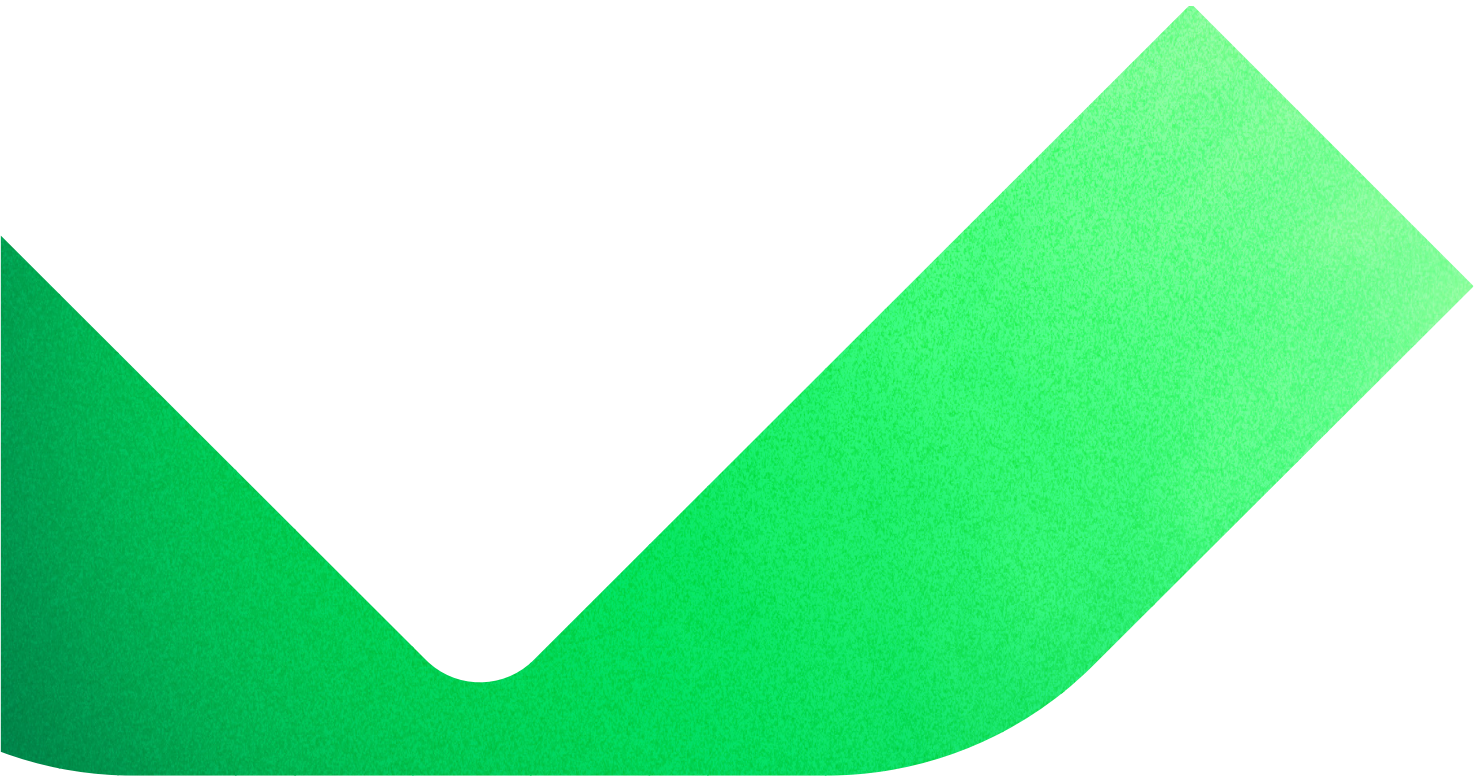
Estensione del modello Zero Trust al backup e al ripristino dei dati

Una guida pratica per i professionisti IT e della sicurezza



Indice

Executive Summary

Zero Trust è una strategia moderna e altamente efficace per proteggere meglio la nostra infrastruttura IT aziendale dal ransomware e da altre minacce. I sistemi di backup e ripristino dei dati sono fondamentali per le nostre imprese e devono essere inclusi in qualsiasi iniziativa Zero Trust.

Tuttavia, Zero Trust può essere complicato da progettare e implementare e, fino ad ora, non c'è stato consenso su come applicarlo al meglio ai sistemi di backup e ripristino dei dati.

Zero Trust Data Resilience (ZTDR), un nuovo modello introdotto da Veeam e Numberline Security, si basa sul modello di maturità Zero Trust della Cybersecurity and Infrastructure Security Agency (CISA). ZTDR estende i principi di Zero Trust al backup e al ripristino, garantendo che le aziende possano ridurre i rischi e raggiungere i propri obiettivi di sicurezza e resilienza.

Seguendo l'approccio alla resilienza dei dati Zero Trust spiegato in questa guida, imparerai cosa cercare in una piattaforma e in un'architettura di backup e ripristino dei dati e sarai in grado di iniziare in modo rapido ed efficace nel tuo ambiente.

Zero Trust : Una breve introduzione

Zero Trust è una moderna strategia di sicurezza basata sull'idea che nessun utente, dispositivo o pacchetto di rete debba essere considerato implicitamente attendibile. Per garantire la sicurezza dei dati, l'accesso alle risorse di dati critiche deve essere segmentato e tutte le comunicazioni devono essere autenticate, valutate e autorizzate prima di concedere qualsiasi accesso. Questo deve essere applicato a ogni segmento e ai relativi dati, applicazioni, risorse o servizi.

Si tratta di un cambiamento significativo rispetto alle tradizionali architetture di sicurezza delle informazioni, che si basavano su perimetri statici basati sulla rete e che chiaramente non sono riuscite a proteggere le nostre imprese dal ransomware e dai malintenzionati.

Presentazione della resilienza dei dati Zero Trust (ZTDR)

I sistemi di backup e ripristino dei dati sono elementi critici dell'IT aziendale, nonché frequenti bersagli di attacchi. Devono essere adeguatamente protetti in modo olistico.

Seguendo i principi ZTDR e scegliendo i fornitori di backup e storage in base alle linee guida ZTDR, la tua azienda otterrà difese più solide, operazioni più efficienti e ripristino più rapido e affidabile.

ZTDR estende i principi fondamentali di Zero Trust

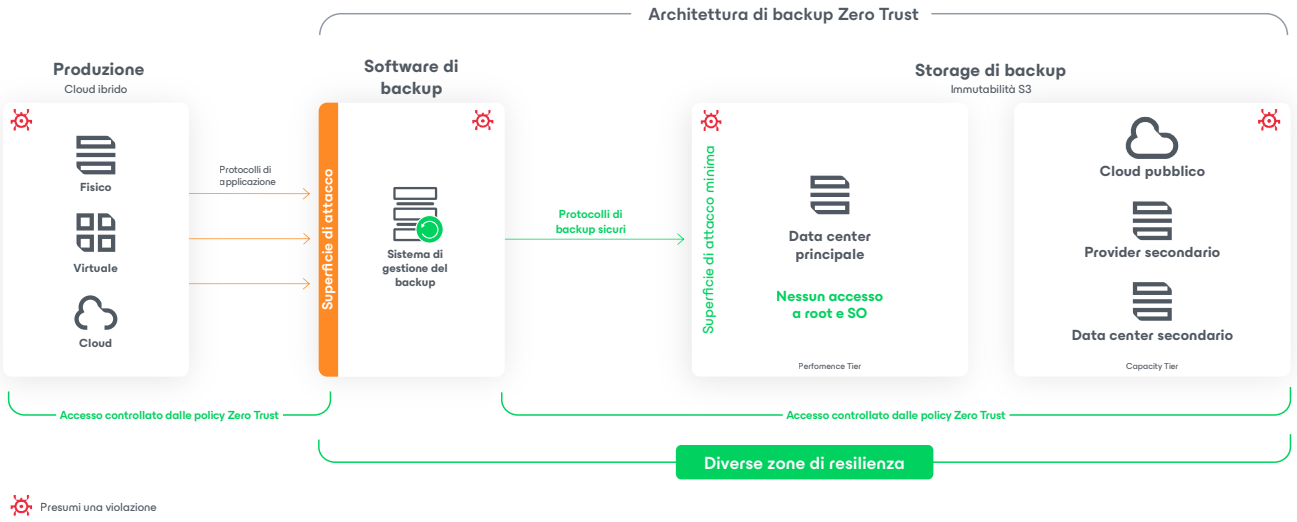
	Separazione tra software di backup e storage di backup	Molteplici Zone di resilienza	Storage di backup immutabile
	Riduzione al minimo della superficie di attacco e del raggio di impatto	Regola 3-2-1 del backup	Proteggere i dati di backup dalla modifica o dall'eliminazione
REQUISITI DELLA SOLUZIONE	Ricerca di soluzioni di backup e ripristino dei dati progettate separando software di backup e storage, e che idealmente impediscono l'accesso root o del sistema operativo allo storage di backup. Queste funzionalità ti consentiranno di applicare rigorosamente i controlli di accesso tramite le policy Zero Trust.	Cerca soluzioni di backup e ripristino dei dati che supportino più zone di resilienza, il che significa che la tua organizzazione può sopravvivere alla perdita o alla compromissione di qualsiasi singolo sistema di backup o ambiente di storage. In questo modo sarai in grado di soddisfare facilmente le linee guida per il backup 3-2-1.	Cerca soluzioni di backup e ripristino dei dati che supportino in modo semplice ed efficiente uno storage di backup immutabile robusto e affidabile. In questo modo avrai la piena certezza che i tuoi dati di backup siano protetti da eliminazione o modifica, anche in presenza di un malintenzionato.

La regola 3-2-1 per le best practice relative al backup:

3	2	1
3 copie dei dati, compresi i dati di produzione.	2 copie dei dati di backup su storage immutabile in zone di resilienza separate.	1 copia in locale.

Architettura di riferimento ZTDR

Questa architettura di riferimento ZTDR mostra come implementare una piattaforma Zero Trust in combinazione con la gestione dei backup e i sistemi di storage.



Guida introduttiva a ZTDR

Sebbene lo Zero Trust sia un percorso, sono disponibili misure immediate e di grande impatto da intraprendere per migliorare la resilienza della sicurezza della tua infrastruttura di backup e ripristino dei dati.

Questa settimana:

Scopri in che misura i tuoi sistemi di backup e ripristino soddisfano i requisiti ZTDR.

Task	Domande da porre
Parla con i team della rete e dell'infrastruttura IT della segmentazione della rete	• Com'è segmentata la nostra rete? • Il software di backup e lo storage di backup sono segmentati in zone di sicurezza separate? • Come viene controllato l'accesso da e verso ciascun segmento dell'infrastruttura di backup?
Valuta se lo storage dei dati di backup è organizzato in più zone di resilienza	• Stiamo seguendo le linee guida del settore sul 3-2-1? • Cosa succede ai nostri processi di backup e ripristino se una delle nostre zone di backup non è disponibile? • Cosa succede ai nostri processi di backup e ripristino se due delle nostre zone di backup non sono disponibili?
Determina se i sistemi di storage di backup sono immutabili in modo appropriato	• In che modo il tuo fornitore di storage documenta e garantisce l'immutabilità? • Un amministratore malintenzionato può modificare le impostazioni di immutabilità o retention utilizzando l'accesso root o del sistema operativo allo storage? • Cosa succede se l'ora di sistema viene portata avanti dolosamente?
Convalida i processi di ripristino	• Cos'è il nostro piano di risposta al disaster recovery? Quando l'abbiamo testato l'ultima volta? • Quante persone del team IT o di storage sono in grado di ripristinare con successo un sistema seguendo i passaggi documentati? • Cosa succede se (persona importante X) non è disponibile durante un incidente?

La settimana prossima:

Convalida i tuoi processi e strumenti, quindi pianifica e crea il consenso per modifiche a breve e medio termine all'infrastruttura e ai processi di backup e ripristino.

Task	Domande da porre
Valuta la tua sicurezza e la ripetibilità dei tuoi processi di ripristino eseguendo test regolari (settimanali/mensili)	• Con quale frequenza eseguiamo i nostri test di ripristino? • Cosa abbiamo imparato sulle lacune nella documentazione o nei processi? • Quando possiamo porvi rimedio?

Task	Domande da porre
Iniziare a pianificare la configurazione di rete, la segmentazione o le modifiche alle regole del firewall	• Con chi, all'interno del team IT o della sicurezza, posso collaborare per individuare potenziali cambiamenti? • Chi nel team di sicurezza sta guidando la nostra iniziativa Zero Trust e come posso supportarla? • Quali modifiche alla segmentazione della rete o all'infrastruttura sono in corso?
Pianifica eventuali modifiche alla configurazione dello storage o valutazioni di nuovi fornitori, al fine di colmare eventuali lacune nell'immutabilità	• Qual è il nostro processo per valutare e procurare storage di backup aggiuntivo? • Che tipo di giustificazione finanziaria, di efficienza o di rischio dovremmo presentare? • Come devo fare per ottenere l'approvazione per avviare un processo di valutazione del fornitore?
Assegnare i proprietari responsabili per eventuali miglioramenti del processo e della documentazione	• Chi sarebbe coinvolto nell'approvazione e nell'attuazione delle modifiche al (processo X)? • Come possiamo fissare un termine di comune accordo per l'implementazione?

Il mese prossimo:

Inizia a implementare le modifiche a breve termine e a identificare eventuali altre modifiche necessarie a lungo termine.

Task	Domande da porre
Implementa i processi di disaster recovery migliorati ed esegui altri test	• Quanto sono migliorati i nostri processi di DR? • Abbiamo colmato tutte le lacune del processo e della documentazione?
Convalida e itera sulla segmentazione della rete	• Quali aree della rete garantiscono ancora un ampio accesso alla rete da e verso i nostri sistemi di backup? • Come possiamo rafforzare questo approccio per migliorare la nostra resilienza al ransomware?
Esegui i miglioramenti alla capacità di storage, alle posizioni e all'immutabilità	• Quanto siamo soddisfatti della nostra capacità di storage di backup? • Quanto siamo sicuri che i nostri sistemi di storage di backup siano immutabili? • In che misura stiamo seguendo i consigli sulle best practice 3-2-1? • In che modo utilizziamo più zone di resilienza?

Cos'altro dovresti cercare?

Convalida proattiva del disaster recovery

Gli incidenti che richiedono il ripristino dei dati di backup si verificano in momenti imprevisti e probabilmente in circostanze di stress elevato. È importante che l'organizzazione disponga di piani e processi di disaster recovery ben compresi, ben documentati e ben collaudati. Assicurati inoltre di avere un elevato livello di fiducia nell'integrità e nella validità dei dati di backup.

Semplicità operativa

Assicurati di selezionare un sistema che sia abbastanza semplice da consentire alla tua organizzazione di operare in modo facile e sicuro, fornendo comunque capacità, scalabilità e sofisticazione sufficienti per soddisfare pienamente le esigenze della tua azienda. Lavora per comprendere chiaramente le capacità e le competenze del tuo personale, in modo che le operazioni non siano lasciate alla buona volontà di un singolo individuo.

Domande frequenti

Zero Trust è qualcosa che puoi acquistare da un fornitore?

No, Zero Trust è qualcosa **che fai tu**: è una strategia di sicurezza che cambia e migliora l'IT, la sicurezza e i risultati aziendali.

Zero Trust riguarda solo la limitazione dell'accesso e la riduzione della produttività degli utenti?

No, il modello Zero Trust consiste nell'eliminare tutti **gli accessi non necessari**, mantenendo al contempo la produttività degli utenti. Molte aziende **migliorano** effettivamente la produttività e l'esperienza utente con Zero Trust.

Perché il modello Zero Trust è importante?

Zero Trust è il modo più efficace per difendere le nostre imprese da rischi come ransomware, malintenzionati e rischi di altro tipo. Dato l'attuale panorama delle minacce, abbiamo la responsabilità di utilizzarlo.

Puoi utilizzare la tua attuale infrastruttura di sicurezza per Zero Trust?

Molto probabilmente, sì! Se utilizzati correttamente, i moderni sistemi firewall, di identità e di infrastruttura possono supportarti all'inizio del tuo percorso Zero Trust. Raggiungere livelli ottimali di maturità Zero Trust può richiedere investimenti aggiuntivi, che possono essere guidati da strumenti come l'architettura di riferimento ZTDR.

Risorse aggiuntive

Vuoi saperne di più su Zero Trust e ZTDR?

- Visita il sito Web di Veeam per leggere la ricerca completa su ZTDR e per scoprire l'approccio di Veeam alla sicurezza dei dati e alla resilienza informatica.
- Per leggere il white paper completo della ricerca ZTDR e conoscere il punto di vista di Numberline Security al riguardo, visita il sito web di Numberline Security.

Informazioni su Veeam Software

Veeam, il leader di mercato #1 al mondo nella resilienza dei dati, ritiene che le aziende debbano controllare tutti i dati quando e dove ne hanno bisogno. Veeam fornisce la resilienza dei dati attraverso il backup, il ripristino, la libertà, la sicurezza e l'intelligence dei dati. Con sede a Seattle, Veeam protegge oltre 550.000 clienti in tutto il mondo che si affidano a Veeam per mantenere operative le loro aziende. Per saperne di più, è possibile visitare www.veeam.com/it o seguire Veeam su LinkedIn @veeam-software e X @veeam.

Maggiori informazioni: veeam.com