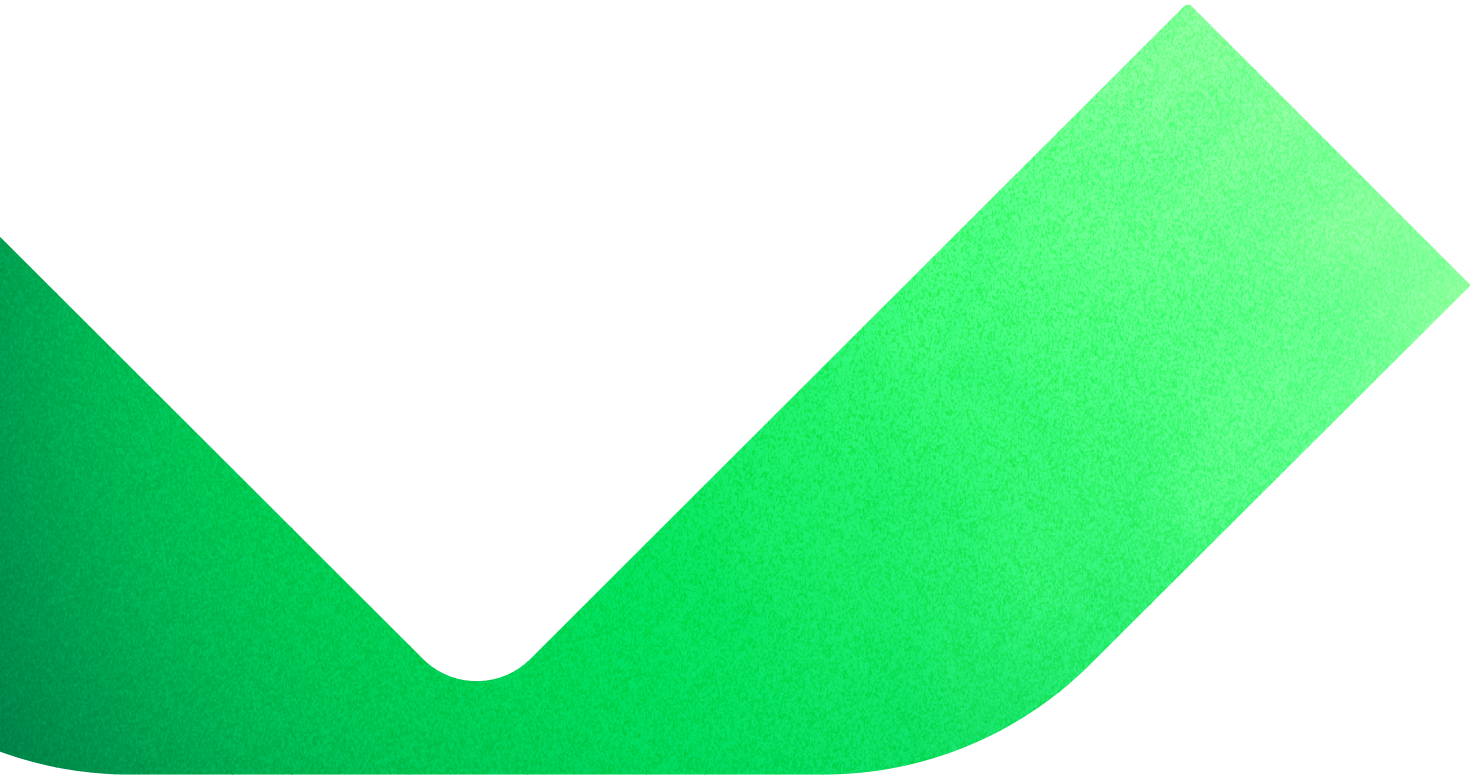
Resilienza dei dati Zero Trust

Un modello per il backup e il ripristino sicuro dei dati



Indice

Executive summary

Le aziende oggi si trovano ad affrontare sfide continue e significative per quanto riguarda la salvaguardia dei dati e delle reti dai malintenzionati, in particolare dagli attacchi ransomware e di esfiltrazione dei dati. Per affrontare queste preoccupazioni, una strategia nota come Zero Trust ha guadagnato un'importanza significativa nel settore della sicurezza delle informazioni ed è ampiamente adottata in ambito enterprise di tutto il mondo.

Tuttavia, anche i modelli Zero Trust più utilizzati mancano di linee guida complete in alcune aree importanti, in particolare per quanto riguarda il backup e il ripristino dei dati. Riconoscendo l'importanza di colmare questa lacuna e applicare i principi Zero Trust a quest'area, introduciamo il concetto di resilienza dei dati Zero Trust. Ciò comprende una serie di requisiti, un'architettura e un'estensione dei modelli di maturità Zero Trust esistenti.

In particolare, le aziende devono utilizzare un sistema di backup e ripristino dei dati che fornisca storage e configurazione dei dati immutabili, applicando al contempo l'accesso contestuale e fortemente autenticato ai dati di origine nei dati di produzione e di backup. Questo sistema deve inoltre supportare senza problemi le architetture ibride comuni nelle aziende moderne e gestire in modo flessibile il ripristino in ambienti diversi.

Implementando un'architettura Zero Trust che soddisfi questi requisiti, le aziende proteggeranno meglio i propri dati, le proprie reti e le proprie applicazioni dai malintenzionati. Zero Trust offre una sicurezza dimostrabilmente migliore rispetto agli approcci tradizionali e le organizzazioni hanno l'obbligo di adottarlo. I nuovi requisiti di resilienza dei dati proposti in questo white paper migliorano ed estendono Zero Trust e dovrebbero essere considerati obbligatori come parte di qualsiasi strategia di sicurezza aziendale.

Introduzione

Zero Trust è una strategia di sicurezza e, per forza di cose, ha una portata ampia. Tuttavia, i modelli e i framework Zero Trust ampiamente utilizzati non includono tutto[1]. Ciò può comportare lacune od omissioni corrispondenti nelle architetture di sicurezza aziendale. In particolare, i sistemi di backup e ripristino dei dati non sono inclusi nei framework Zero Trust comunemente utilizzati. Questa è una lacuna spiacevole, poiché i dati enterprise sono molto spesso l'obiettivo principale dei malintenzionati sia negli attacchi ransomware che in quelli di esfiltrazione dei dati.

I sistemi di backup e ripristino dei dati sono elementi critici dell'IT enterprise e come tali devono essere trattati. Hanno accesso in lettura a tutto ciò che è importante per eseguirne il backup. Devono anche essere in grado di scrivere dati negli ambienti di produzione per svolgere la loro funzione di ripristino dei dati. Contengono inoltre una copia completa dei dati aziendali più importanti. Nel loro insieme, tutti questi attributi sottolineano l'importanza dei sistemi di backup e ripristino dei dati ed evidenziano il loro valore come bersaglio per i malintenzionati.

Naturalmente, i sistemi di backup e ripristino dei dati fanno parte della responsabilità dell'IT da decenni, ma spesso non sono stati inclusi nell'ambito o nella responsabilità dei team di sicurezza. Tuttavia, dato il livello e la sofisticazione delle minacce alla sicurezza che le aziende devono attualmente affrontare, adottare solo una prospettiva di rete e infrastruttura IT per il backup e il ripristino dei dati non è più sufficiente. In pratica, ci siamo imbattuti in aziende in cui questi sistemi erano mal configurati e non monitorati, causando quindi rischi significativi.

Una sicurezza moderna ed efficace si basa sui principi Zero Trust, quindi è arrivato il momento di dare un nuovo sguardo ai sistemi di backup e ripristino dei dati attraverso questa lente. Questo whitepaper raggiunge questo obiettivo proponendo un nuovo concetto di resilienza dei dati Zero Trust. Adottando questo approccio, le imprese avranno un percorso chiaro e concreto per avere difese più forti, operazioni più efficienti e ripristino più rapido.

[1] Il documento CISA ZTMM afferma che "Mentre lo ZTMM copre molti aspetti della sicurezza informatica critici per le imprese federali, non affronta altri aspetti della sicurezza informatica come... il ripristino".

Approccio

I classici elementi fondamentali della sicurezza delle informazioni — la triade CIA di riservatezza, integrità e disponibilità — sono tutti applicabili al backup e al ripristino dei dati. Le aziende devono evitare l'esfiltrazione dei dati (riservatezza), impedire al ransomware di crittografare i dati (integrità) e garantire che i sistemi siano protetti dagli attacchi e possano essere ripristinati rapidamente dopo un attacco (disponibilità).

I principi fondamentali di Zero Trust sono certamente rilevanti per questo dominio e dovrebbero essere applicati all'accesso ai sistemi IT degli utenti e delle aziende, nonché ai sistemi di backup e ripristino dei dati. Questi principi includono l'eliminazione della fiducia implicita e delle reti non segmentate, il controllo di tutti gli accessi da parte di policy dinamiche e contestuali tramite i Policy Enforcement Point (PEP), la richiesta di un'autenticazione adeguatamente forte di tutti i soggetti, presumendo una violazione, e la garanzia e la convalida dell'integrità del sistema e dei dati. In questo white paper, vedremo come questi principi confluiscono nel nuovo set di requisiti proposto per un'architettura di resilienza dei dati Zero Trust.

Il framework che rappresenta lo standard de facto per esaminare la maturità di Zero Trust è il modello di maturità Zero Trust CISA[2] raffigurato nella Figura 1, che definisce cinque pilastri principali: Identità, Dispositivi, 1 Reti, Applicazioni e carichi di lavoro, Dati. Definisce inoltre tre capacità trasversali: Visibilità e analisi, automazione e orchestrazione, governance.

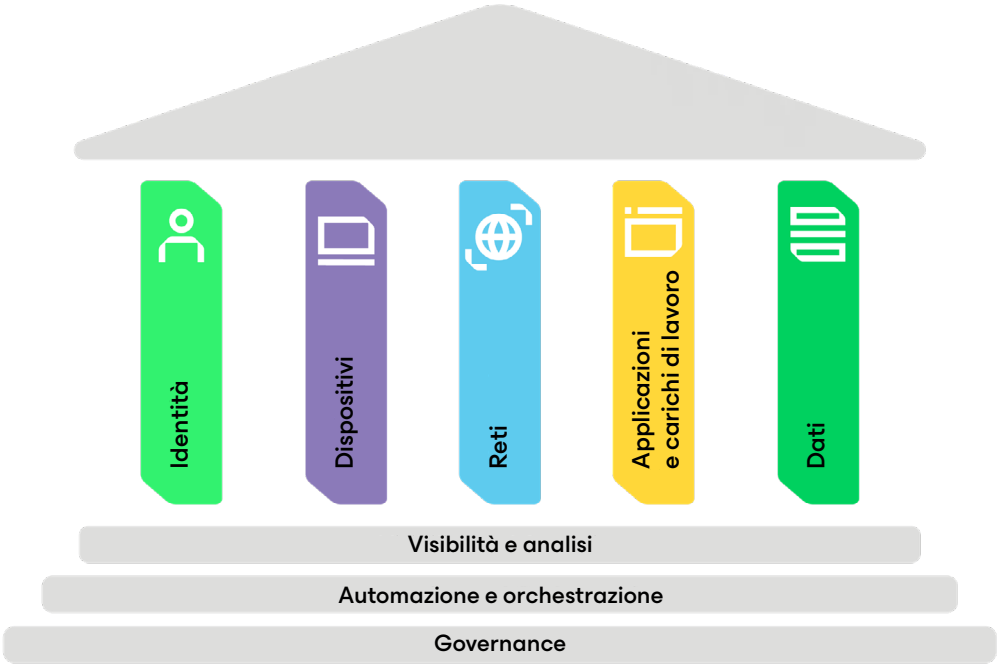


Figura 1: Modello di maturità Zero Trust del CISA

[2] https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

All'interno del pilastro Dati, il modello CISA identifica cinque funzioni dettagliate, con capacità e attributi previsti per ciascun livello di maturità.

Tuttavia, all'interno di queste funzioni, l'argomento dell'integrità e del ripristino del backup dei dati è minimamente trattato e CISA indirizza i lettori a un documento NIST del 2020 non collegato a Zero Trust. In sintesi, il modello Zero Trust CISA tace sui requisiti e sui livelli di maturità per i sistemi di backup e ripristino dei dati. Poiché quest'area è così importante per la riservatezza, l'integrità e la disponibilità dell'enterprise, riteniamo che questa lacuna debba essere colmata.

A tal fine, stiamo introducendo il concetto di resilienza dei dati Zero Trust, che include principi, un'architettura di riferimento e un nuovo set di capacità per il modello di maturità Zero Trust. Nel loro insieme, rappresentano un'estensione e un miglioramento di Zero Trust e si tradurranno in una posizione di sicurezza aziendale più forte.

Le funzioni sono:

- Gestione dell'inventario dei dati
- Categorizzazione dei dati
- Disponibilità dei dati
- Accesso ai dati
- Crittografia dei dati

Resilienza dei dati Zero Trust: Principi

I principi fondamentali di Zero Trust Data Resilience (ZTDR) sono:

Accesso con privilegio minimo

Immutabilità

Resilienza del sistema

Convalida proattiva

Semplicità operativa

Discutiamo ciascuno di questi uno per uno.

Accesso con privilegio minimo

Questo principio è fondamentale per Zero Trust ed è una parte obbligatoria di qualsiasi architettura Zero Trust. Tuttavia, vale la pena esaminarne l'applicabilità alle specifiche della ZTDR (Zero Trust Data Resilience), poiché si applica a più livelli. Dal punto di vista della rete, il sistema di gestione del backup deve essere isolato sulla rete in modo che nessun utente o dispositivo non autenticato o non autorizzato possa accedervi. Allo stesso modo, il sistema di storage di backup deve essere isolato. Ciò impedisce ai malintenzionati di scoprire entrambi i sistemi attraverso la ricognizione della rete o sfruttando una vulnerabilità.

L'accesso legittimo e autorizzato al sistema di backup deve avvenire solo tramite un punto di applicazione delle policy Zero Trust (PEP) con un'autenticazione avanzata appropriata e controlli della postura del dispositivo. Il PEP Zero Trust deve inoltre controllare l'accesso ai dati di origine (ovvero i dati di cui viene eseguito il backup), con un'autenticazione appropriata e un certo livello di convalida del dispositivo o del sistema per garantire che sia il sistema di gestione del backup a leggere i dati di produzione, anziché un sistema o un processo dannoso.

Anche l'accesso dal sistema di gestione dei backup allo storage di backup deve essere controllato da un PEP e segmentato dal resto della rete con un'autenticazione forte appropriata. Si noti che rivisiteremo questo requisito nel diagramma dell'architettura sottostante, poiché è importante: il sistema di storage di backup deve essere segmentato dal sistema di gestione del backup.

Immutabilità

Il concetto e l'esigenza di dati di backup immutabili sono stati ampiamente adottati negli ultimi anni, in concomitanza con l'aumento della prevalenza e della sofisticazione del ransomware. Un backup immutabile è definito come un backup dei dati che utilizza un meccanismo di storage che, una volta scritto, non può essere modificato. La premessa è che, anche se un malintenzionato fosse presente sulla rete e in grado di assumere il controllo del sistema di backup e avere accesso allo storage di backup, non sarebbe in grado di eliminare o modificare (crittografare) i dati di backup. Parte dell'immutabilità deriva dalle proprietà fisiche dei supporti di storage, ad esempio i dischi ottici Write-Once-Read-Many, mentre tecnologie più recenti utilizzano supporti con immutabilità applicata a livello hardware, firmware o software. Più di recente, i principali provider di servizi cloud hanno aggiunto funzionalità di storage immutabile per soddisfare i requisiti di conformità e archiviazione aziendali.

NOTA

I requisiti di immutabilità si estendono oltre ai dati memorizzati e devono includere anche i periodi di retention dei dati. Alcuni dati immutabili possono essere configurati per lo storage indefinito, mentre altri possono avere un periodo di retention definito, ad esempio uno o cinque anni. I dati che superano il periodo di conservazione possono essere eliminati, quindi il sistema di storage dei dati deve anche rendere immutabile il periodo di conservazione dei dati. In questo modo si elimina la riduzione dolosa dei periodi di retention.

Resilienza del sistema

Abbiamo una visione abbastanza ampia della resilienza del sistema e riteniamo che debba essere applicata non solo all'infrastruttura di backup stessa, ma all'intero ecosistema di strumenti, tecnologie e processi relativi al backup e al ripristino dei dati. In particolare, l'infrastruttura di backup deve essere resiliente a guasti e attacchi, come l'indisponibilità di componenti o reti o la manipolazione del Network Time Server (NTP) per far scadere i dati di backup in modo dannoso. Deve inoltre essere facile configurare l'uso di uno storage dei dati di backup distribuito ed eterogeneo, ad esempio tra aree geografiche o tipi di infrastruttura. La resilienza viene inoltre migliorata separando i dati di backup dal sistema di gestione dei backup, in modo che la compromissione del sistema di backup non comprometta anche lo storage dei dati. Cerca infatti un sistema di gestione dei backup che, in caso di compromissione o guasto, possa essere ricostituito senza influire sulla tua capacità di accedere e ripristinare i dati di backup.

Il sistema deve inoltre essere resiliente ai cambiamenti previsti e imprevisti nell'ambiente aziendale. Le modifiche previste includono l'aggiunta o la rimozione pianificata di componenti dell'infrastruttura, compresa l'adozione di applicazioni e dati ibridi o basati sul cloud. Ovvero il sistema di backup deve essere in grado di acquisire e archiviare in modo efficiente i dati aziendali, indipendentemente dalla posizione di origine o dalla tecnologia. Le modifiche impreviste si verificano in genere durante la risposta agli incidenti o il disaster recovery (DR) e sono spesso classificate come supporto per il ripristino in ambienti diversi. Quando un'organizzazione ripristina i dati, è del tutto possibile che l'ambiente di ripristino sia in esecuzione in una posizione o in un tipo di infrastruttura diverso. Ad esempio, un data center on-premises allagato potrebbe richiedere il ripristino in un ambiente basato su cloud, con le operazioni che proseguono lì per un periodo di tempo prolungato. Pertanto, il sistema di backup deve supportare sia il ripristino in un ambiente diverso sia nuovi backup da questo ambiente di produzione in futuro.

Il sistema di storage dei dati di backup stesso, oltre a fornire uno storage dei dati immutabile, dovrebbe essere facilmente rafforzato. Ciò può assumere la forma di un'appliance pre-rafforzata o di un sistema configurabile dall'amministratore con chiare raccomandazioni sul rafforzamento, che sarà più adatto ad aziende sofisticate.

Convalida proattiva

Per garantire il corretto funzionamento del sistema è necessario monitorarlo e convalidare tutti gli aspetti funzionali e i processi. Questo ha due aspetti. In primo luogo, il sistema di backup dovrebbe essere monitorato in termini di rete, prestazioni e sicurezza. Cioè, questo sistema dovrebbe essere trattato come qualsiasi altro sistema di produzione ad alto valore.

In secondo luogo, e soprattutto, la validità dei dati di backup - e l'affidabilità e l'efficacia dei processi di ripristino - devono essere regolarmente convalidati. Per definizione, il ripristino dei dati di backup avverrà in momenti inaspettati e probabilmente in un ambiente ad alto stress. È importante che l'organizzazione abbia un processo ben compreso, ben documentato e ben collaudato. Devono inoltre essere presenti più persone in grado di eseguire questo compito per tenere conto delle ferie, dell'indisponibilità e del turnover del personale.

Tieni presente che, sebbene ciò richieda un investimento di tempo ed energie, dimostra maturità operativa ed è una "polizza assicurativa" in caso di disastro. Inoltre, tieni presente che "disastro" non significa necessariamente un disastro letterale o un evento importante come l'allagamento di un data center. Ad esempio, un'azienda con cui abbiamo lavorato ha riscontrato un flusso di lavoro automatizzato fuori controllo a causa di un errore di programmazione, che ha comportato l'eliminazione di quantità significative di dati di produzione nel sistema di gestione finanziaria. Non si è trattato di un disastro in senso letterale, e si è evitato che diventasse un disastro potenziale utilizzando i processi di ripristino dei dati (convalidati).

Inoltre, il sistema di gestione dei backup dovrebbe avere la capacità diretta o indiretta di organizzare i backup in una sequenza temporale di infezione da malware. Ovvero, dovrebbe essere in grado di rilevare (o essere informato di) infezioni da malware e classificare i backup come puliti, discutibili o compromessi, a seconda di quando sono stati acquisiti.

NOTA

I processi di convalida e ripristino dei dati devono inoltre rispettare i requisiti di privacy e residenzialità dei dati. Tutto ciò può aggiungere complessità e rischi, quindi deve essere eseguito in modo ponderato, conoscendo sia il contenuto dei dati sia gli obblighi legali e di conformità dell'organizzazione.

Semplicità operativa

Il nostro principio finale è la semplicità operativa, che definiamo come un sistema abbastanza facile da gestire per la tua organizzazione, pur fornendo capacità, scalabilità e sofisticazione sufficienti per soddisfare pienamente le esigenze della tua azienda. Ovvero, un sistema adeguato alla tua organizzazione.

Questo è importante: abbiamo visto aziende faticare a utilizzare e rendere operativi sistemi troppo complessi per le dimensioni, il team, le competenze e le esigenze della loro organizzazione. Ciò si traduce in vantaggi limitati, frustrazione e incapacità di garantire la maturità della sicurezza o valore aziendale. Una serie di attributi da ricercare in un fornitore di backup è la sua forza relativa a livello di orchestrazione e automazione. I fornitori con solide capacità nelle loro piattaforme saranno più veloci e più facili da rendere operativi.

Concludendo questa sezione, ognuno di questi principi è integrato nel nuovo modello di maturità descritto più avanti in questo documento e sarà anche evidente nell'architettura di riferimento che discuteremo in seguito.

Resilienza dei dati Zero Trust: Architettura di riferimento

Le architetture di backup dei dati variano necessariamente da un'azienda all'altra, data l'enorme variabilità delle infrastrutture di rete, applicative e dei dati, tra gli altri fattori. Ciononostante, esistono elementi architettonici comuni a causa dei principi Zero Trust comuni, che devono essere presenti in qualsiasi architettura di resilienza dei dati Zero Trust.

La nostra architettura di riferimento è illustrata nella Figura 2 e illustra i requisiti chiave in questo tipo di sistema. Si noti che descrive l'ambiente dal punto di vista del sistema di gestione dei backup. Anche l'accesso regolare e quotidiano degli utenti e dei sistemi ai sistemi di produzione sarebbe controllato dalle PEP Zero Trust, ma questo aspetto viene omesso nel diagramma per maggiore chiarezza.

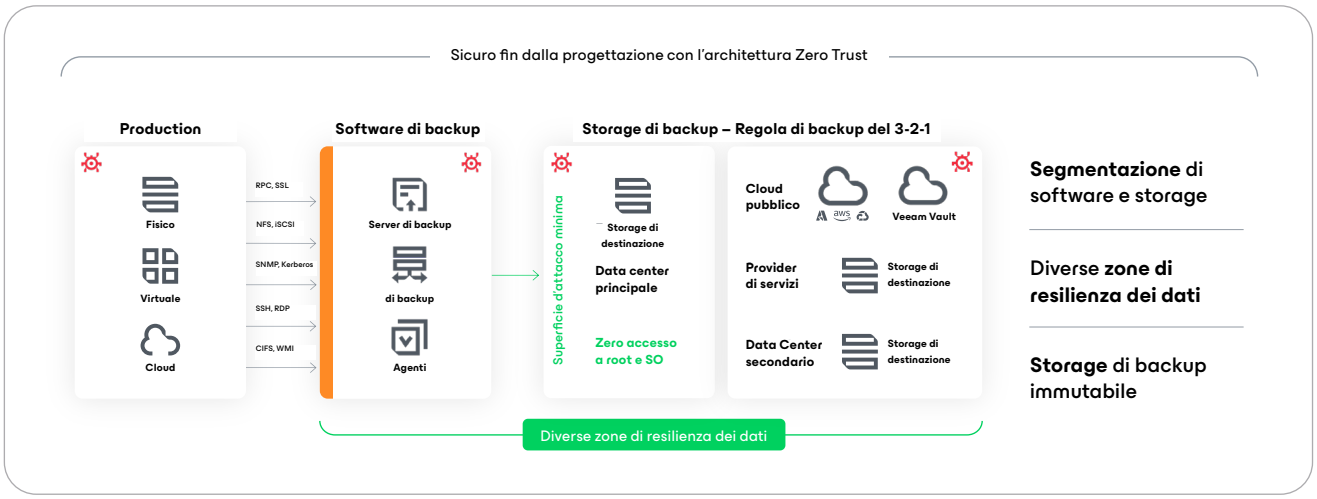


Figura 2: Resilienza dei dati Zero Trust: Architettura di riferimento

Innanzitutto, prendi nota delle parti fondamentali di qualsiasi architettura Zero Trust: il Policy Decision Point (PDP) centralizzato, che delega l'autenticazione dell'identità al sistema Identity and Access Management (IAM) aziendale. Il PDP si basa sull'archivio criteri per prendere decisioni di accesso per le identità autenticate, incluse le identità umane e non personali (di sistema). In questa architettura, il PDP prende le decisioni sull'accesso al sistema di gestione dei backup. Queste decisioni vengono comunicate tramite il piano di controllo (mostrato da linee tratteggiate) con i Policy Enforcement Points (PEP), che si collocano logicamente in linea tra il sistema di gestione del backup e le origini dei dati di cui eseguire il backup e le posizioni di backup di destinazione.

L'architettura include anche una struttura consigliata per i dati di cui è stato eseguito il backup. Oltre al requisito di immutabilità dei dati, le aziende dovrebbero mirare a mantenere almeno una copia in una posizione primaria, con una connessione di rete a bassa latenza verso il sito di ripristino previsto. Ciò consente snapshot di backup rapidi, che incoraggiano punti di ripristino più frequenti e tempi di ripristino più rapidi. Naturalmente, la posizione primaria è spesso collocata insieme ai sistemi di produzione, quindi la nostra architettura di riferimento illustra anche l'obiettivo di avere almeno 2 copie dei dati in posizioni secondarie[3]. Queste devono essere 1 geograficamente isolate dalla posizione principale per ottenere la resilienza a un disastro regionale. Il probabile compromesso è una connessione di rete più lenta, che può comportare punti di ripristino a frequenza inferiore e tempi di ripristino più lunghi.

NOTA

Il sistema di gestione dei backup è volutamente separato dai suoi livelli di storage. Ciò consente al sistema di backup di distribuire senza problemi i dati di backup su più repository immutabili e geograficamente distribuiti. Consente inoltre alle aziende di selezionare repository di storage di backup che offrono la migliore combinazione di prestazioni, prezzo e semplicità operativa per le loro specifiche esigenze. Fornisce inoltre un ulteriore livello di sicurezza controllando la comunicazione tramite un PEP.

[3] Esistono varie scuole di pensiero sul numero di backup in diverse posizioni, spesso indicate tramite diciture mnemoniche come 3-2-1 o 3-2-1-1-0.

Resilienza dei dati Zero Trust: Modello di maturità esteso

Sebbene i principi e l'architettura di riferimento che abbiamo proposto per la resilienza dei dati Zero Trust siano universalmente applicabili, non possono essere applicati completamente e immediatamente nella maggior parte delle aziende. Come la maggior parte degli aspetti di Zero Trust, devono essere pianificati e adottati in modo incrementale. Il modo standard per modellare e comunicare questo è attraverso un modello di maturità. Come accennato nell'introduzione, stiamo seguendo il framework che è lo standard de facto CISA Zero Trust Maturity Model e lo stiamo estendendo con quattro funzioni nuove che comprendono i nostri principi e requisiti.

Queste nuove funzioni sono:

Accesso ai dati e ai sistemi aziendali

Accesso allo storage di backup e ai dati

Resilienza del sistema

Monitoraggio e convalida del sistema

Queste estensioni ZTDR del modello di maturità sono illustrate nelle Figure da 3 a 6, che mostrano come ciascuna delle quattro nuove funzioni dovrebbe essere avanzata nei livelli di maturità standard: Tradizionale, Iniziale, Avanzato e Ottimale.

Per ognuna delle funzioni, abbiamo identificato gli attributi previsti per ogni livello di maturità. Il modello descrive quindi i miglioramenti e i cambiamenti che un'organizzazione deve apportare per progredire nella maturità di ciascuna funzione. Successivamente, esaminiamo ciascuna delle funzioni una per una, passando attraverso i livelli di maturità.

Accesso ai dati e ai sistemi aziendali

Questa funzione è definita come i mezzi e i meccanismi attraverso i quali il sistema di gestione del backup (BMS) ha accesso ai dati di origine di cui è incaricato di eseguire il backup.

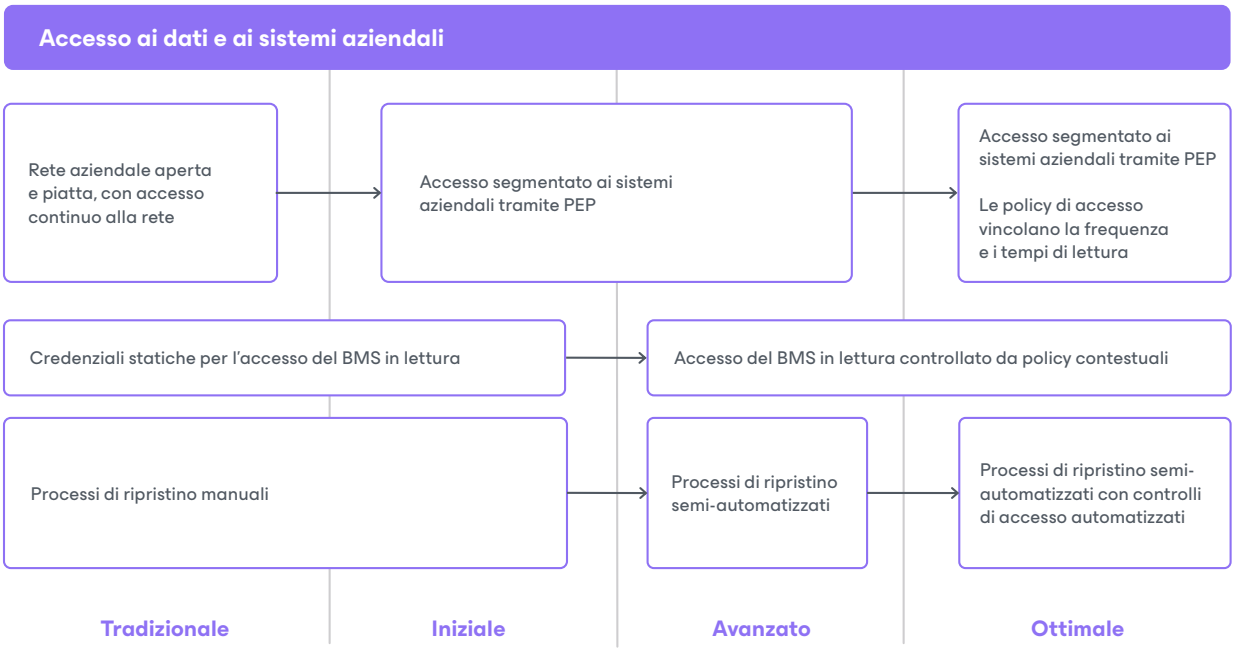


Figura 3 — Accesso ai dati e ai sistemi aziendali: Modello di maturità

Al livello di maturità **Tradizionale**, l'azienda dispone di una rete piatta e aperta e il sistema di gestione dei backup dispone di un accesso di rete continuo e senza ostacoli ai sistemi di origine. Il BMS utilizza credenziali statiche, come una chiave API, un nome utente/password memorizzato o un certificato, per autenticare e leggere i dati di origine. Quando l'azienda utilizza il BMS per ripristinare un sistema, si affida a processi manuali.

Per passare al **Livello iniziale**, l'azienda deve iniziare ad applicare una migliore segmentazione della rete e limitare l'accesso del BMS ai sistemi aziendali tramite un punto di applicazione della policy Zero Trust, introducendo il principio del privilegio minimo.

Quando l'azienda è al livello **Avanzato**, avrà introdotto le policy di accesso contestuali per l'accesso del BMS ai dati e ai sistemi aziendali, utilizzando così meglio le funzionalità di applicazione dinamica delle policy Zero Trust. Avranno anche iniziato a utilizzare processi di ripristino automatizzati con alcuni passaggi manuali per l'avvio e la convalida del processo.

Al livello **Ottimale**, l'organizzazione avrà migliorato l'utilizzo delle policy di accesso, per vincolare l'accesso del BMS solo ai periodi di tempo consentiti o agli eventi di ripristino attivi. In questo modo si applica ulteriormente il principio del privilegio minimo.

Accesso allo storage di backup e ai dati

Questa funzione è definita come i mezzi e i meccanismi attraverso i quali il sistema di gestione del backup ha accesso in scrittura e lettura allo storage di backup e ai dati in esso memorizzati.

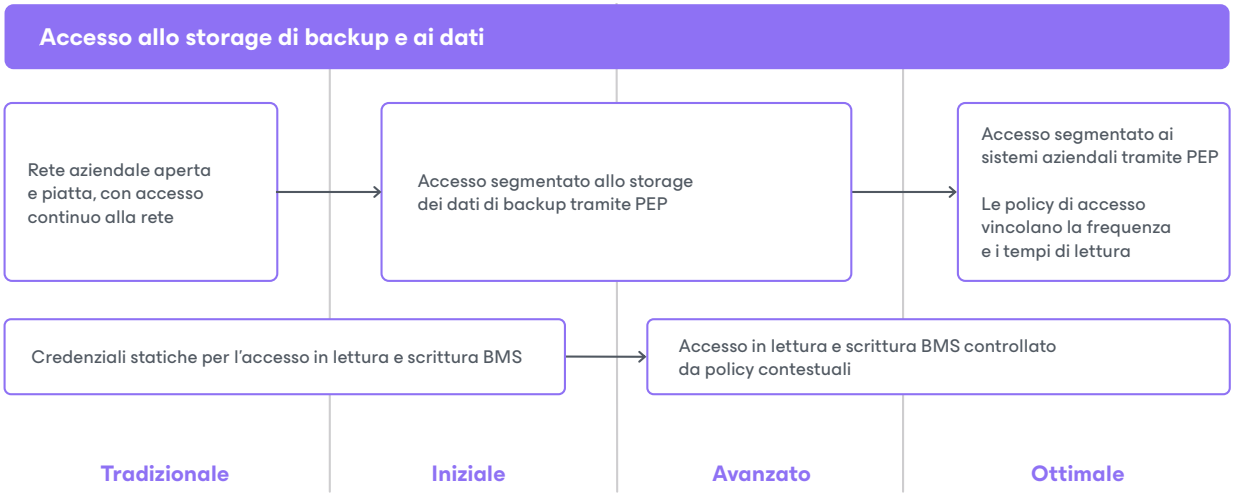


Figura 4 — Accesso allo storage di backup e ai dati: Modello di maturità

Al livello di maturità **Tradizionale**, l'azienda dispone di una rete piatta e aperta e il sistema di gestione dei backup dispone di un accesso di rete continuo e senza ostacoli al sistema di storage di backup e ai dati di backup in esso archiviati. Il BMS utilizza credenziali statiche, ad esempio una chiave API, un nome utente/password memorizzato o un certificato, per autenticarsi e scrivere nello storage e leggere i dati memorizzati.

Per passare al livello **Iniziale**, l'azienda deve iniziare ad applicare una migliore segmentazione della rete e a limitare l'accesso del BMS allo storage di backup e ai dati archiviati tramite un punto di applicazione della policy Zero Trust, applicando il principio del privilegio minimo.

Quando l'azienda raggiunge il livello **Avanzato**, saranno state introdotte delle policy di accesso contestuali per l'accesso del BMS allo storage di backup e ai dati archiviati. In questo modo è possibile sfruttare al meglio le capacità di applicazione dinamica delle policy all'interno dell'azienda.

Al livello **Ottimale**, l'organizzazione avrà migliorato l'utilizzo delle policy di accesso, per vincolare l'accesso del BMS allo storage solo ai periodi di tempo consentiti o durante eventi di ripristino attivi. In questo modo si applica ulteriormente il principio del privilegio minimo.

Resilienza del sistema

Questa funzione è definita come le caratteristiche del sistema di backup in relazione alla resistenza ai guasti del sistema, ai guasti dei componenti o alle attività dannose.

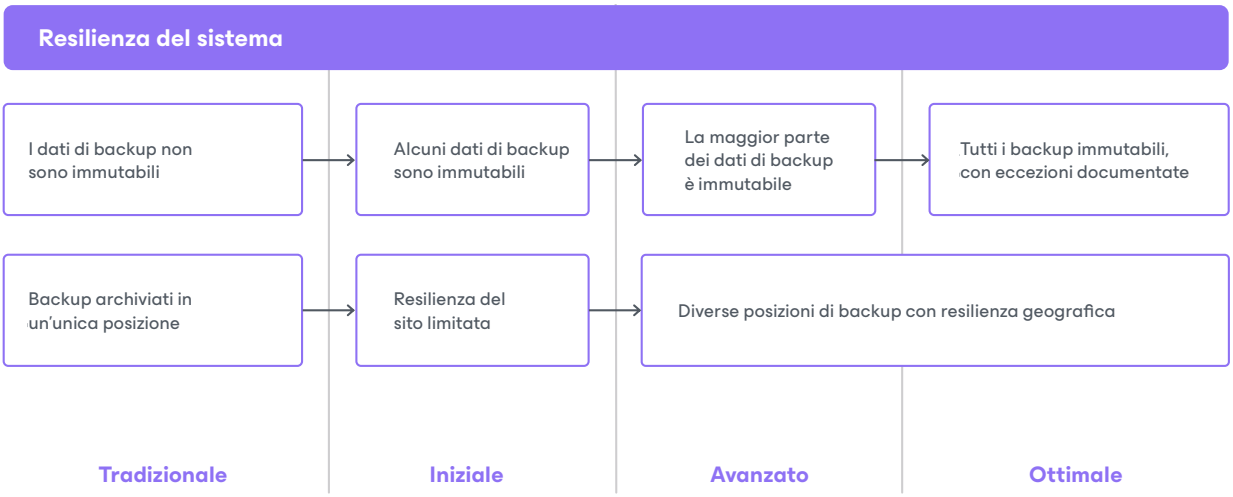


Figura 5 — Resilienza del sistema: Modello di maturità

Al livello di maturità **Tradizionale**, l'organizzazione utilizza uno storage modificabile per i dati di backup, mettendone a rischio l'integrità e la disponibilità. Inoltre, in genere archiviano i backup in un'unica posizione, esponendo così l'organizzazione a una perdita completa in caso di disastro regionale.

Man mano che l'organizzazione passa al livello **Iniziale**, deve iniziare a utilizzare lo storage immutabile per alcuni dei backup dei dati e introdurre una resilienza limitata della posizione per tali backup.

Al livello **Avanzato**, l'organizzazione utilizzerà principalmente lo storage di backup immutabile, idealmente dando priorità in base alla sensibilità e alla criticità dei dati. Avranno inoltre introdotto e reso operativo l'uso di più posizioni di storage di backup, in aree geografiche distribuite.

Quando l'azienda raggiunge il livello **Ottimale**, sarà passata all'utilizzo completo dello storage di backup immutabile, con eventuali eccezioni documentate e approvate. Per impostazione predefinita, le nuove origini dati e le nuove applicazioni utilizzeranno il backup immutabile. Questo livello fornisce all'organizzazione la massima resilienza contro i disastri regionali e i malintenzionati.

Monitoraggio e convalida del sistema

Questa funzione comprende gli strumenti e i processi con cui l'azienda assicura che il proprio sistema di gestione dei backup e lo storage di backup funzionino correttamente e che sia in grado di eseguire un processo di ripristino quando necessario.

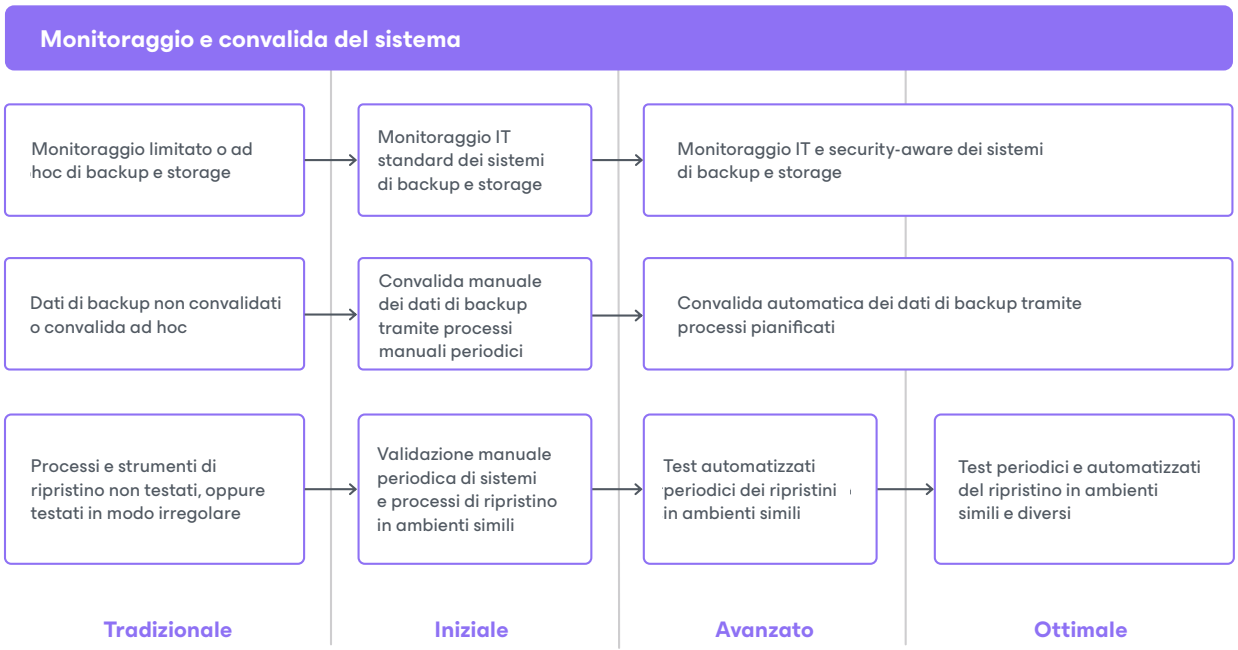


Figura 6 — Monitoraggio e convalida del sistema: Modello di maturità

Al livello di maturità **Tradizionale**, l'azienda esegue solo il monitoraggio di base dell'infrastruttura di backup e storage, riflettendo spesso una minore maturità informatica e operativa complessiva. L'organizzazione potrebbe non verificare i dati di backup o eseguire solo controlli periodici (ovvero manuali e poco frequenti). Inoltre, l'azienda non testerà regolarmente gli strumenti e i processi di ripristino per renderli ben compresi, documentati e ripetibili.

Al livello **Iniziale**, avrà adottato un livello standardizzato di monitoraggio informatico e operativo del sistema di backup e storage. Istituirà inoltre la convalida regolare dei dati di backup tramite processi manuali. Avrà anche implementato una convalida regolare (manuale) dei processi di ripristino per garantire la conoscenza istituzionale e la familiarità con essi.

Al livello **Avanzato**, le organizzazioni avranno implementato strumenti e processi di monitoraggio sia informatico che di sicurezza per i sistemi di backup e storage. Inoltre, convalideranno automaticamente i dati di backup con controlli pianificati che segnalano e inoltrano qualsiasi risultato anomalo. Questo includerà il test automatizzato degli strumenti e dei processi di ripristino in ambienti simili alla produzione.

Al livello **Ottimale**, l'organizzazione avrà migliorato la sofisticazione dei propri test di ripristino per testarli per il ripristino in ambienti diversi.

Riepilogo del modello di maturità

Nel loro complesso, queste nuove funzioni definiscono un insieme di capacità e un insieme previsto di competenze mappate tra i quattro livelli di maturità Zero Trust. Forniscono una roadmap e una guida pratica per le aziende che desiderano integrare i propri sistemi di backup e ripristino dei dati nell'iniziativa Zero Trust.

Conclusione

Zero Trust è un modo migliore di affrontare la sicurezza delle informazioni e, in qualità di leader della sicurezza, abbiamo l'obbligo di portare questa strategia nelle nostre aziende. Le attuali architetture Zero Trust e i modelli di maturità sono solidi punti di partenza, ma sono incompleti. In particolare, i requisiti e gli approcci dei dati di backup e ripristino sono assenti.

Tradizionalmente le aziende hanno trattato il backup e il ripristino come se fossero di competenza dell'IT, ma la prevalenza del ransomware e la digitalizzazione quasi completa del business richiedono che i responsabili della sicurezza ampliano il loro ambito di applicazione per includere questo aspetto.

In questo white paper abbiamo introdotto il concetto di resilienza dei dati Zero Trust, con una serie di principi fondamentali, un'architettura di riferimento ed estensioni del modello di maturità Zero Trust. Riteniamo che, adottando questo approccio di resilienza dei dati Zero Trust, le aziende avranno un percorso chiaro e concreto verso delle difese più forti, delle operazioni più efficienti e un ripristino più rapido. I dati aziendali sono troppo importanti per non applicare le best practice di sicurezza, e Zero Trust è il modo più efficace per farlo.

Informazioni su Veeam Software

Veeam®, il leader di mercato #1 al mondo nella resilienza dei dati, ritiene che ogni azienda dovrebbe essere in grado di fare un balzo in avanti dopo un'interruzione con la sicurezza e il controllo di tutti i dati, quando e dove ne ha bisogno. Veeam la chiama resilienza radicale e ci impegniamo al massimo per creare modi innovativi per aiutare i nostri clienti a raggiungerla. Le soluzioni Veeam sono progettate appositamente per migliorare la resilienza dei dati garantendo backup, ripristino, libertà, sicurezza e intelligence dei dati. Con Veeam, i responsabili IT e della sicurezza hanno la tranquillità di sapere che le loro applicazioni e i loro dati sono protetti e sempre disponibili negli ambienti cloud, virtuali, fisici, SaaS e Kubernetes. Con sede a Seattle e uffici dislocati in oltre 30 Paesi, Veeam protegge più di 550.000 clienti in tutto il mondo, incluso il 74% delle aziende Global 2000, che si affidano a Veeam per mantenere operativi i propri business. La resilienza radicale inizia con Veeam. Per saperne di più, è possibile visitare www.veeam.com o seguire Veeam su LinkedIn @veeam-software e X @veeam.

Maggiori informazioni:
veeam.com/it