



veeam

I tuoi primi
100 giorni
con Veeam Data Platform

Guida per i leader alla resilienza misurabile

La maggior parte delle organizzazioni ritiene di essere protetta, ma poche lo hanno verificato.

In un recente sondaggio, il 90% dei leader della sicurezza ha dichiarato di poter ripristinare entro i propri obiettivi definiti. Tuttavia, tra le vittime di ransomware, solo il 28% ha ripristinato completamente i propri dati (Fonte: [Data Trust and Resilience Report 2026](#)). La fiducia non è la stessa cosa della comprovata capacità di ripristino, e il divario tra le due è ciò che permette ai ransomware di prevalere, agli audit di fallire e alle interruzioni di servizio di trasformarsi in crisi.

Perché la resilienza è reale solo quando la si può dimostrare.

Questa Guida adotta un approccio strategico all'implementazione di Veeam Data Platform. Mentre il tuo team lavora sulle [tappe fondamentali dell'implementazione tecnica](#), questa Guida le traduce in risultati aziendali: i rischi ridotti, le capacità acquisite e le prove che avrai a disposizione alla fine.

Perché le decisioni in merito alla tolleranza al rischio, agli impegni di ripristino e alla Business Continuity spettano a te. Questa Guida illustra le tue responsabilità e ciò che sarai in grado di comunicare con sicurezza al consiglio di amministrazione, ai revisori dei conti e alle compagnie assicurative entro il centesimo giorno.

Ecco cosa ti offre questa Guida:

1. I cinque risultati che distinguono la resilienza comprovata dalla protezione presunta
2. Cosa significa per il tuo ruolo: CIO, CISO o CFO
3. I sette casi d'uso coperti dal tuo investimento e come la loro attivazione determina il tuo ritorno sull'investimento (ROI)
4. Le domande che vale la pena porre al proprio team per confermare che la resilienza perduri dopo il centesimo giorno

90%

dei leader della sicurezza ha dichiarato di poter ripristinare entro gli obiettivi definiti

28%

delle vittime di ransomware hanno ripristinato completamente i propri dati



Dall'esposizione all'evidenza: i cinque risultati che contano

Questi sono i cinque risultati a cui la tua organizzazione si impegna quando implementa Veeam Data Platform. Ognuno rappresenta una fase che conduce dall'esposizione alla prova, e insieme delineano le caratteristiche di un ambiente resiliente e verificabile.

01. Implementato

Sai esattamente cosa è protetto, dove risiede e secondo quale Standard. Nessuna supposizione e nessuna mancanza scoperta sotto pressione.



02. Protetto

Ogni carico di lavoro critico è coperto da un piano su cui la strategia di Business Continuity può contare. Nulla viene trascurato quando conta di più.



03. Rinforzato

Un attaccante non può compromettere la tua capacità di ripristino. Copie immutabili sia in locale che off-site ti garantiscono un punto di ripristino pulito, indipendentemente da come si evolve un incidente.



04. Ripristinabilità verificata

Puoi dimostrare che il ripristino funziona, non solo affermarlo. È testato, documentato e pronto per essere presentato al consiglio di amministrazione, ai revisori dei conti e all'assicuratore.



05. Efficienza operativa

La resilienza non dipende da una sola persona o da un singolo atto eroico. Si basa su responsabilità chiare, reportistica strutturata e una cadenza definita che il team può sostenere.



Cosa significa questo per il tuo ruolo:



CIO/CTO

Quando il consiglio chiede se la tua organizzazione può ripristinare da un incidente grave, avete una risposta testata e documentata. Il rischio di interruzione del servizio non è più una questione di fiducia; è una questione di documentazione.



CISO

Hai un punto di ripristino pulito e confermato prima che un incidente si trasformi in una crisi, non dopo. La scansione delle minacce, le copie immutabili e i risultati dei test documentati forniscono le prove richieste da assicuratori, revisori dei conti e team legale.



CFO

L'idoneità all'assicurazione cyber, i termini di rinnovo e le trattative sui premi migliorano quando la recuperabilità è comprovata anziché semplicemente presunta. La ricerca dimostra che le organizzazioni con investimenti più solidi nella resilienza dei dati hanno pagato un riscatto solo nel 33% dei casi, contro il 52% di quelle prive di tali investimenti. Il tuo investimento in Veeam è mirato, prevedibile e direttamente finalizzato a ridurre l'esposizione finanziaria causata da un'interruzione del servizio non pianificata.



33%

dei casi in cui le organizzazioni con maggiori investimenti nella resilienza dei dati hanno pagato un riscatto.

52%

delle organizzazioni prive di tali investimenti hanno pagato un riscatto.

Fonte: [Rapporto sulla fiducia e la resilienza dei dati \(2026\)](#).

Il valore sbloccato

Il valore offerto da Veeam Data Platform va ben oltre un singolo ruolo o un singolo incidente. A partire dai primi 100 giorni, la tua organizzazione acquisirà capacità che rispondono alla reale complessità degli ambienti IT moderni: infrastrutture ibride, espansione del cloud, pressione normativa e un panorama delle minacce in continua evoluzione.

Questi sono i sette casi d'uso che il tuo investimento è destinato a coprire.

Protezione e ripristino

In caso di incidente, la qualità della risposta dipende dalla qualità della preparazione. Questo è lo standard fondamentale di cui ogni organizzazione ha bisogno, indipendentemente dal settore o dall'infrastruttura.

1. **Rilevamento e risposta alle minacce:** Veeam esegue la scansione delle catene di backup per rilevare indicatori di malware e controlla l'integrità dei file prima del ripristino, così la tua organizzazione può ripristinare in sicurezza anziché reintrodurre una minaccia. I risultati documentati delle scansioni supportano il processo di Incident Response e soddisfano i requisiti degli assicuratori.
2. **Disaster Recovery nel cloud:** quando l'infrastruttura on-premises si guasta, Veeam sposta i carichi di lavoro verso destinazioni cloud entro gli obiettivi di ripristino definiti. Il tuo team dispone di un piano collaudato e attuabile, invece di un processo manuale che non funziona bene sotto pressione.



Controllo e conformità

La pressione normativa e i requisiti in materia di controllo completo dei dati si stanno espandendo. La tua strategia di protezione dei dati deve tenere il passo. Se operi in un settore regolamentato o ti stai preparando a un ciclo di audit, questo è il punto su cui concentrarsi per primo.

3. **Governance, risk e conformità:** Veeam produce report conformi alle esigenze di audit di cui i team di conformità e legali hanno bisogno, inclusi i risultati dei test di ripristino, l'inventario della copertura e la conferma della policy di retention, senza richiedere la raccolta manuale delle evidenze durante l'audit.
4. **Sovranità:** Veeam garantisce alla tua organizzazione il pieno controllo su dove i dati di backup vengono conservati ed elaborati, rispettando i requisiti di residenza dei dati nelle varie giurisdizioni senza compromettere la capacità di ripristino.



Operare attraverso la complessità

L'infrastruttura moderna non risiede in un unico luogo. Nemmeno la tua strategia di protezione dovrebbe esserlo. Se sei nel pieno di una migrazione o già operate in ambienti Multi-Cloud o SaaS ibridi, è qui che si concentra il rischio operativo.

5. **Mobilità dei carichi di lavoro tra ambienti:** man mano che i carichi di lavoro migrano tra ambienti on-premises, cloud ed edge, Veeam assicura che la protezione li segua. La copertura non si interrompe in caso di modifiche all'infrastruttura.
6. **Protezione Multi-Cloud:** Veeam garantisce capacità di protezione e ripristino coerenti tra i Provider cloud, eliminando il rischio operativo derivante da strumenti frammentati e lacune tra le piattaforme.
7. **SaaS ibrido:** i dati critici contenuti nelle applicazioni SaaS sono protetti insieme ai carichi di lavoro della tua infrastruttura, colmando così il gap di copertura che la maggior parte delle organizzazioni scopre solo dopo un incidente.

Non si tratta di capacità future o di componenti aggiuntivi facoltativi. Sono i vantaggi che la tua organizzazione acquisisce durante la fase di implementazione e attivazione, ognuno dei quali riduce una specifica categoria di rischio e offre al tuo team di leadership fiducia nei momenti di maggiore pressione. La questione non è se la tua organizzazione abbia bisogno di questo livello di resilienza, ma con quale rapidità puoi raggiungerlo.



Giorno 100 non è il traguardo. È la baseline di riferimento. La resilienza è una pratica, non un progetto.

Veeam offre la [Veeam DataAI Command Platform](#), il comprovato [Data & AI Trust Maturity Model](#) e le [competenze tecniche](#) necessarie per guidare il tuo team dalla prima implementazione fino alla piena dimostrazione della resilienza. Siamo qui per aiutarti in ogni fase del percorso.

Assicurati che il tuo team abbia la [Guida tecnica ai primi 100 giorni](#) e inizia ad allineare ambito di implementazione, timeline e risultati attesi.

La resilienza a questo livello non è un'ambizione a lungo termine. Con il giusto piano di implementazione, è una realtà a breve termine per la tua organizzazione.

La prossima mossa spetta a te.

Domande che vale la pena rivolgere periodicamente al team

- ✓ Sono coperti tutti i carichi di lavoro critici e sono state affrontate eventuali lacune o guasti nella protezione?
- ✓ Quando abbiamo testato per l'ultima volta un ripristino completo in condizioni reali, e abbiamo risultati documentati che lo dimostrino?
- ✓ Se fossimo colpiti da un ransomware stanotte, potremmo identificare un punto di ripristino pulito e ripristinare senza pagare un riscatto?
- ✓ Le nostre funzioni di conformità e legale possono produrre evidenze di audit senza intervento manuale? Inoltre, la nostra architettura è ancora conforme agli obblighi normativi attuali?
- ✓ Chi dispone di accesso amministrativo al nostro ambiente di backup e quando è stata effettuata l'ultima revisione?



Informazioni su Veeam Software

Veeam è l'azienda di fiducia per dati e IA, specializzata nell'aiutare le organizzazioni a garantire che i loro dati e la loro IA siano pienamente compresi, protetti e resilienti, al fine di accelerare l'adozione di un'IA sicura su larga scala. In qualità di leader di mercato nella resilienza dei dati e nella gestione della postura di sicurezza dei dati, Veeam è progettata per la convergenza di identità, dati, sicurezza e rischi legati all'intelligenza artificiale. Con sede centrale a Seattle e uffici in oltre 30 paesi, Veeam protegge oltre 550.000 clienti in tutto il mondo, tra cui l'82% delle aziende Fortune 500. Maggiori informazioni su www.veeam.com oppure segui Veeam su LinkedIn [@veeam-software](https://www.linkedin.com/company/veeam) e X [@veeam](https://twitter.com/veeam).

➔ Maggiori informazioni: [veeam.com](https://www.veeam.com)