Resilienza al ransomware nel 2022

Il backup di livello enterprise è la tua ultima linea di difesa

Dave Russell,

Vice President, Enterprise Strategy, Veeam Software

Jeff Reichard,

Vice President, Public Sector & Compliance Strategy, Veeam Software

Chris Hoff,

Data Protection & Ransomware Marketing Manager, Veeam Software

Indice

Le aziende non possono prevenire un attacco informatico

La crescita e l'evoluzione del ransomware è una delle tendenze più distruttive dell'ultimo decennio. Questa esplosione ha trasformato il ransomware da un crimine economico a un crimine con immense implicazioni per la sicurezza globale. La NATO, il governo federale USA, l'esercito degli Stati Uniti e il G7 hanno recentemente riconosciuto la gravità della minaccia ransomware e la necessità di una risposta coordinata su ampia scala da parte dei governi e dell'industria.

Le imprese non possono prevenire un attacco informatico, ma devono adottare le misure necessarie per essere preparate a proteggere efficacemente i propri dati quando si verifica.

Crescita del ransomware 2016-2021

Costo globale:
da 325 milioni a

20 miliardi di USD

Frequenza:
da ogni 2 minuti a ogni

11 secondi

Innovazione:

Bitcoin,
ransomware-as-a-service,
estorsione doppia/tripla

Il backup sicuro è la tua ultima linea di difesa

La soluzione di disponibilità implementata dovrebbe essere in grado di proteggere tutti i carichi di lavoro d'importanza critica.

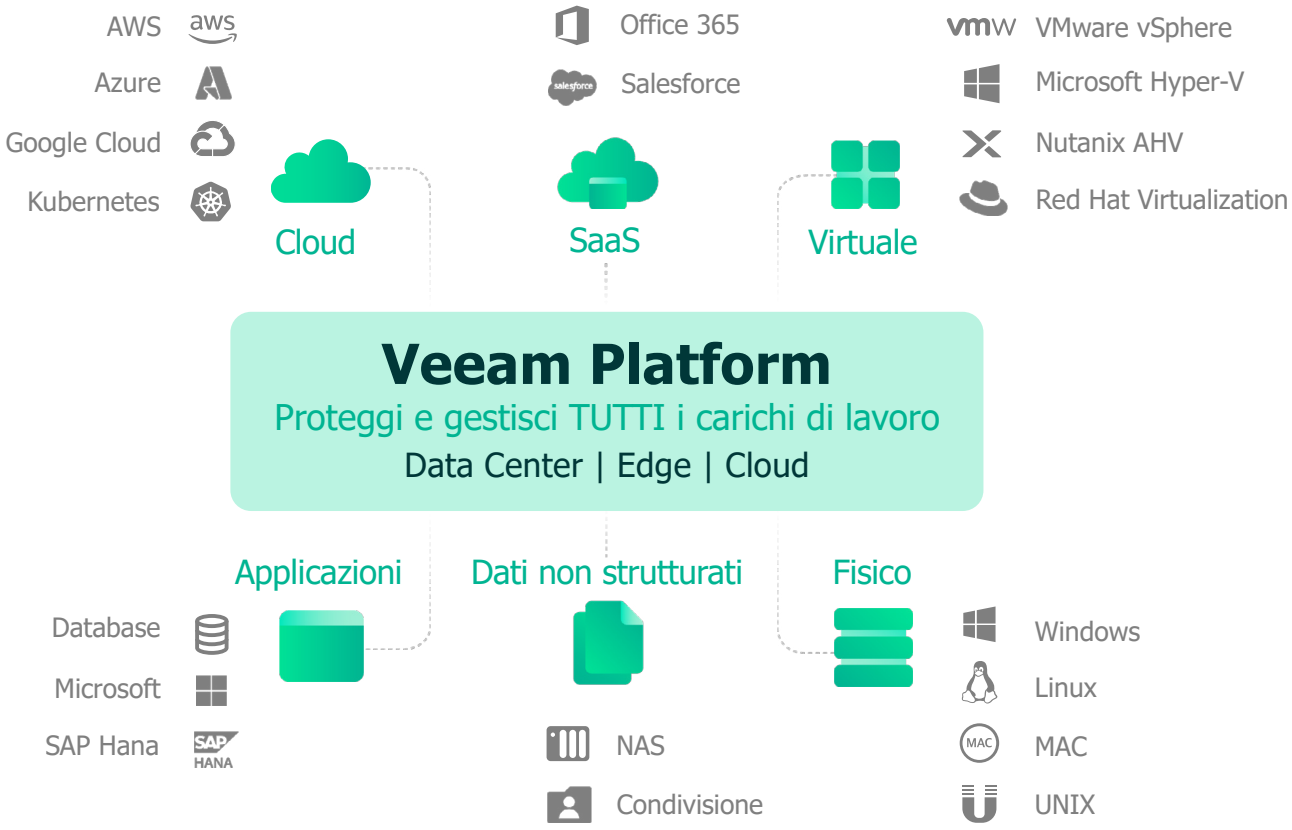
Indipendentemente dal fatto che i carichi di lavoro vengano implementati on-premises, nel cloud con IaaS oppure come SaaS, i dati d'importanza critica ora risiedono in molte posizioni e devono essere trasferibili per tenere conto dei requisiti futuri. La piattaforma di protezione dovrebbe avere la capacità di scalare, a seconda dei requisiti e dei carichi di lavoro da proteggere. La soluzione di backup dovrebbe essere in grado di acquisire dati tramite una moltitudine di metodi, inclusi backup, replica, Continuous Data Protection (CDP) e integrazioni di array storage.

La Veeam® Platform offre tutte queste funzionalità, consentendo una soluzione che si adatta e si estende man mano che la tua azienda e i suoi requisiti si evolvono nel tempo.

L'approccio di Veeam è modulare ed estensibile, senza soluzioni separate, nessuna dipendenza dall'hardware e nessuna preoccupazione di crescere troppo per la soluzione.

Le capacità di rimedio dal ransomware software-defined di Veeam funzionano con qualsiasi infrastruttura, oggi e in futuro.

Non dovrebbe essere necessaria un'infrastruttura proprietaria, consentendo quindi all'azienda di implementare l'hardware o il cloud che preferisce. La flessibilità dell'infrastruttura non solo consente a un'organizzazione di determinare l'hardware sul quale viene eseguita la propria soluzione di backup, ma anche di proteggere i backup dal ransomware, indipendentemente da dove risiedono i dati essenziali.

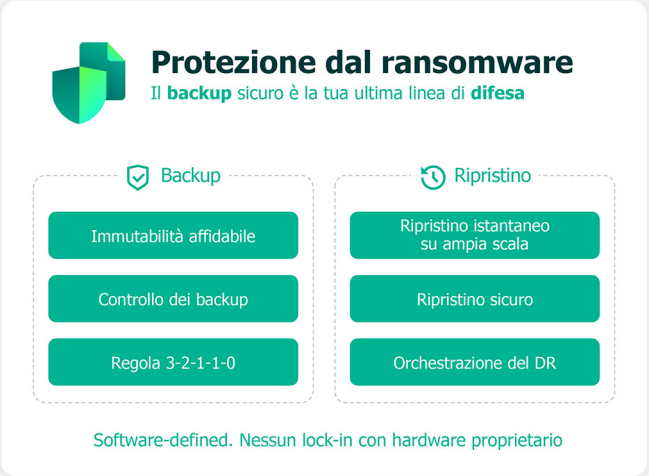


Costruire un framework enterprise per un ripristino resiliente

I programmi di sicurezza efficienti richiedono una struttura per capire cosa deve essere protetto e il valore della risorsa per l'organizzazione per determinare come deve essere implementata la protezione. Indipendentemente dalla metodologia scelta dalle aziende, il framework deve definire risultati misurabili che consentano ai team IT di difendersi dagli attacchi e di ripristinare rapidamente nel caso di un attacco riuscito.

Senza un metodo strutturato per gestire il rischio di sicurezza informatica, sarebbe facile concentrare tutti gli sforzi allestendo difese basate sul rilevamento come firewall e antivirus, trascurando però i processi e gli strumenti imprescindibili per rispondere in modo efficace e ripristinare da un attacco andato a segno. In altre parole, il miglior attacco è una solida difesa che comprenda la predisposizione di una robusta strategia di backup e protezione dei dati e dei carichi di lavoro. I backup riusciti sono l'ultima linea di difesa dagli attacchi informatici e possono essere il fattore decisivo per prevenire notevoli interruzioni, la perdita di dati e il pagamento di un costoso riscatto.

Con questa prospettiva, abbiamo realizzato questa guida alle best practice per fornire consigli provenienti dal mondo reale sulla protezione dei dati.



1. Immutabilità affidabile

Ora i criminali informatici tentano regolarmente di crittografare o eliminare i backup di un'organizzazione come parte di qualsiasi attacco ransomware. Il successo per l'avversario è fondamentale in questo caso, perché senza backup, la vittima deve pagare profumatamente per ripristinare i propri dati.

I backup resilienti sono semplicemente backup che non possono essere distrutti da un avversario, anche se ha acquisito le credenziali amministrative.

Veeam offre un approccio infallibile basato su policy per la gestione dei dati attraverso varie opzioni di storage resilienti. A migliorare la resilienza complessiva, le soluzioni di storage certificate fornite da Veeam e tramite il nostro ampio ecosistema di partner garantiscono l'*immutabilità* (l'impossibilità di cancellare o modificare i dati per un tempo prescritto). **Queste opzioni comprendono il nostro repository con protezione avanzata Veeam, che offre una solida opzione immutabile per i backup on-premises.** Se preferisci tenere i tuoi dati nel cloud, Veeam fornisce l'immutabilità utilizzando AWS Amazon S3 e altri provider di object storage compatibili con S3 approvati, sfruttando la capacità di blocco degli oggetti.

I backup scritti su uno storage resiliente saranno una delle difese più critiche per garantire la resilienza dal ransomware. Uno storage di backup resiliente significa avere una o più copie dei dati di backup su una qualsiasi combinazione dei seguenti supporti:

- Backup su nastro
  (e rimosso dalla libreria o contrassegnato come WORM)
- Backup immutabili in object storage S3
  o compatibili con S3
- Supporti fisicamente isolati e offline
  (unità rimovibili, unità rotanti)
- Backup in Veeam Cloud Connect con Insider Protection
  (una funzionalità del fornitore dei servizi)
- Backup immutabili in un repository con
  protezione avanzata

2. Controllo dei backup

Una strategia di difesa informatica solida e completa inizia sempre con backup validi. Disporre di backup affidabili, verificati e testati è il primo passo per il successo di qualsiasi ripristino. I team IT, sempre impegnati, hanno bisogno di un modo per verificare automaticamente l'integrità dei dati di backup nel momento in cui vengono acquisiti. In caso di problemi, è possibile acquisire un altro backup mentre i dati di produzione sono ancora disponibili, garantendo così l'assenza di problemi scoperti dopo che i dati di produzione non sono più disponibili, sono stati compromessi o sono considerati inaffidabili e non integri.

Veeam SureBackup® è il pioniere della verifica del backup automatizzata, e questa è una funzionalità chiave delle nostre best practice per la resilienza dal ransomware. SureBackup attiva automaticamente server e applicazioni in un ambiente isolato dalla rete ed esegue verifiche dello stato che comprendono molte modalità integrate di controllo delle applicazioni, come l'esecuzione di specifici comandi Active Directory o SQL per verificare l'integrità dell'applicazione. La funzionalità di test automatizzato può essere estesa e personalizzata per soddisfare le tue esigenze e può essere programmata per l'esecuzione quando lo ritieni più appropriato, con l'invio contestuale di un report sullo stato nella tua casella di posta una volta terminato il test.

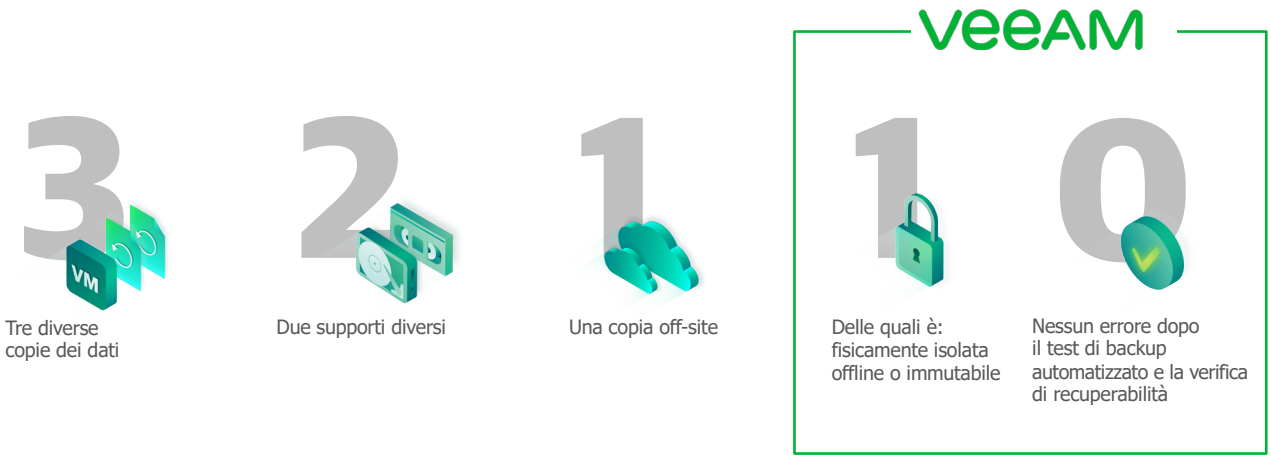
3. Regola 3-2-1-1-0

Veeam consiglia di seguire la regola 3-2-1-1-0, un nostro miglioramento alla ben nota regola del settore 3-2-1.

Da molti anni Veeam promuove la regola 3-2-1 come strategia di gestione dei dati complessiva. La regola 3-2-1 consiglia di conservare almeno tre copie dei dati importanti su almeno due differenti tipi di supporto, con almeno una di queste copie mantenuta off-site.

All'avanzare della minaccia ransomware, Veeam ha sottolineato che almeno "una" copia dei dati deve essere resiliente (ovvero fisicamente isolata, offline o immutabile). Questa raccomandazione è imprescindibile per la resilienza al ransomware.

La moderna applicazione della regola 3-2-1-1-0 risponde alla necessità del requisito della copia resiliente ed è uno dei concetti più importanti che un'organizzazione può implementare per essere meglio preparata a respingere e a porre rimedio alle minacce informatiche.



4. Ripristino istantaneo su ampia scala

Prima del ransomware, in genere le organizzazioni ripristinavano solo il 3-5% dei dati di backup nell'arco di un anno. Con un attacco ransomware in corso, però, il 100% dei dati di produzione può essere crittografato o contaminato da malware e quindi è necessario recuperarli tutti velocemente. L'accesso rapido ai dati è fondamentale, con l'obiettivo di avere più una ripresa che un ripristino per tutte le operazioni essenziali.

Veeam ha introdotto per prima il ripristino istantaneo nel 2010 e, da allora, ha ridefinito ed esteso questa capacità.

Oggi Veeam è ottimizzato per ripristinare in modo rapido più macchine contemporaneamente, per gestire anche le più pressanti esigenze di ripristino enterprise.

Veeam offre il ripristino istantaneo dei dati:

- Senza richiedere costosi dispositivi proprietari o unità a stato solido
- Senza limitarsi ai soli dati di backup più recenti

5. Ripristino dei dati sicuro

Basandosi sulla funzionalità di ripristino istantaneo menzionata in precedenza, Veeam si integra con le principali soluzioni anti-malware per fornire un processo di ripristino automatizzato per controllare e pulire i dati di backup infetti, garantendo che i dati di backup ripristinati in produzione siano privi di minacce informatiche, eliminando le reinfezioni.

Veeam Secure Restore offre agli utenti una fase di scansione antivirus opzionale e completamente integrata come parte integrante di qualsiasi processo di ripristino scelto.

Questa funzionalità risolve i problemi associati alla gestione del malware dannoso con la possibilità di garantire che tutti i dati di copia che si desidera o che è necessario ripristinare in produzione siano in buono stato e privi di malware. **Il ripristino sicuro è un altro metodo innovativo, in attesa di brevetto, per rimediare a un attacco derivante da un malware nascosto nei dati di backup.**

6. Orchestrazione del DR

Sia chiaro, gli attacchi informatici sono disastri. In un'emergenza, il team ha bisogno di risultati automatizzati e ripetibili. Il tuo set di strumenti deve consentire test e verifiche regolari della velocità con cui potresti ripristinare da un disastro, inclusi test automatizzati dell'accessibilità e dell'usabilità di server e applicazioni dopo il ripristino. E il processo di test e i risultati dovrebbero essere documentati automaticamente per soddisfare il consiglio di amministrazione e i revisori della sicurezza esterni.

Veeam Disaster Recover Orchestrator, **lo strumento leader di settore di Veeam, consente di automatizzare completamente e documentare i flussi di lavoro complessi, inclusi i test di ripristino su larga scala senza interruzioni con documentazione dinamica.**

Ripristino affidabile

- Orchestrazione scalabile e affidabile
- Incentrato sull'applicazione

Test automatizzati

- Senza interruzioni
- Pianificati e on-demand
- Controlli del preparato

Documentazione dinamica

- Audit trail
- Reportistica di conformità
- Tracciamento modifica integrato
- Rimedio proattivo

Conclusioni

La risposta dell'azienda a minacce come il ransomware richiede una strategia di rimedio completa. L'ampio set di difese contro i ransomware di Veeam offre il set di funzionalità più completo sul mercato. Lo facciamo adottando un approccio software-first che ti offre la flessibilità di mantenere uno storage resiliente e immutabile on-premises e nel cloud senza rimanere vittima del lock-in nell'hardware proprietario. La piattaforma Modern Data Protection di Veeam può aiutarti a raggiungere la resilienza digitale e ridurre al minimo le interruzioni dopo un attacco ransomware.

Che i tuoi dati risiedano on-premises o nel cloud, è fondamentale disporre di un set completo di capacità di rimedio dal ransomware. L'integrazione di queste best practice nel tuo programma di sicurezza semplifica la risposta agli attacchi informatici ed evita la perdita di dati o il pagamento di un costoso riscatto.

Informazioni su Veeam Software

Veeam® è il leader nelle soluzioni di backup, ripristino e gestione dei dati che forniscono la Modern Data Protection. Veeam offre una singola piattaforma per ambienti cloud, virtuali, SaaS, Kubernetes e fisici. I nostri clienti sono sicuri che dati e applicazioni sono protetti e sempre disponibili con la piattaforma più semplice, flessibile, affidabile e potente del settore. Veeam protegge oltre 400.000 clienti in tutto il mondo, tra cui oltre l'82% delle aziende Fortune 500 e oltre il 60% delle Global 2.000. L'ecosistema globale di Veeam comprende oltre 35.000 partner tecnologici, rivenditori, provider di servizi e partner Alliance, con uffici in oltre 30 Paesi. Per maggiori informazioni, visita www.veeam.com oppure segui Veeam su LinkedIn @veeamsoftware e Twitter @veeam.

Informazioni sugli autori

Dave Russell è Vice President of Enterprise Strategy.

Jeff Reichard è Vice President of Public Sector and Compliance Strategy.

Chris Hoff è un Data Protection & Ransomware Marketing Manager.

Soluzioni Veeam per le tue pratiche di rimedio dal ransomware

- Veeam Availability Suite
- Veeam Backup *for Microsoft 365*
- Veeam Disaster Recovery Orchestrator

Ulteriori informazioni sulle capacità relative al ransomware di Veeam sono disponibili su questo sito Web dedicato:
https://www.veeam.com/ransomware-protection.html

Scopri di più sulle soluzioni di backup aziendale qui:
un approfondimento delle capacità di sicurezza informatica di Veeam è disponibile all'indirizzo:
https://www.veeam.com/enterprise-backup-solutions-software.html