OBJECT FIRST

Lista di controllo

Checklist: resilienza al ransomware

Riconoscere lo storage di backup con immutabilità assoluta

Gli attacchi ransomware hanno raggiunto un livello di sofisticazione mai visto prima. Il 66% delle organizzazioni negli ultimi due anni ha subito almeno un attacco, che nel 96% dei casi ha preso di mira i dati di backup.*

Ciò significa che quando (perché è praticamente sicuro) si verifica una violazione che rischia di compromettere la tua attività, reputazione e carriera, uno storage di backup immutabile è la tua linea di difesa più sicura ed efficace.

Tuttavia, se i dati "immutabili" possono essere sovrascritti da un amministratore di backup o di storage, un fornitore o un aggressore, allora non si tratta di una soluzione di storage con immutabilità assoluta.

Usa questa lista di controllo in 3 passaggi per verificare se la tua soluzione di backup attuale (o futura) è resiliente al ransomware.

*Ricerca ESG 2025

Preparati

Passaggio 1: utilizzo dello Storage a oggetti S3

- ☐ La tua soluzione di storage usa il blocco e il controllo delle versioni degli oggetti S3 per garantire l'immutabilità e preservare la cronologia dei backup?
- ☐ La soluzione applica la modalità di conformità (non la modalità di governance) e supporta la crittografia end-to-end dal momento stesso in cui i dati vengono creati?
- ☐ L'immutabilità può essere verificata in modo indipendente tramite standard aperti e test di penetrazione di terzi indipendenti?

Solo lo storage a oggetti S3 garantisce una sicurezza intrinseca, grazie all'integrazione nativa dell'immutabilità direttamente nel suo protocollo e nelle sue API. Questo design di base garantisce che, una volta scritti, i dati non possano essere modificati o eliminati. Lo storage a oggetti S3 si basa su un'architettura aperta e standard del settore, che segue le migliori pratiche di sicurezza IT e consente i test di terze parti.

Passaggio 2: garanzia di Immutabilità immediata

- ☐ La tua soluzione rende i dati di backup immutabili non appena vengono scritti, senza ritardi o passaggi intermedi?
- ☐ Evita l'immutabilità basata su snapshot o sul livello deduplicazione, che applica le protezioni solo dopo il completamento del lavoro?
- ☐ I dati di backup vengono scritti direttamente nello storage a oggetti con il blocco oggetti S3 abilitato?

Garantire che i dati di backup siano immutabili dal momento stesso in cui vengono scritti è fondamentale per prevenire alterazioni non autorizzate, mantenere l'integrità dei dati e difendersi dal ransomware. Il modo comprovato e più sicuro per ottenere questo risultato è attraverso il versioning S3 combinato con il blocco oggetti, che garantisce l'immutabilità dell'oggetto fin dalla sua creazione nel sistema di storage.

Passaggio 3: utilizzo di un dispositivo di destinazione specializzato

- ☐ La tua configurazione separa rigorosamente il software di backup dallo storage di backup, limitando l'impatto di una violazione?
- ☐ Stai utilizzando un dispositivo di destinazione dedicato gestito dal fornitore anziché una configurazione di storage fai da te che richiede aggiornamenti manuali, patch e monitoraggio?
- ☐ La tua soluzione è verificabilmente sicura o si basa su un file system proprietario del fornitore che impedisce i test indipendenti e nasconde come viene applicata l'immutabilità?

Per storage di backup specializzato si intende un dispositivo di storage autonomo configurato e ottimizzato per lo storage dei dati di backup. Ne esistono due tipi: dispositivi integrati, che combinano il software di backup e storage in un unico sistema; e dispositivi di destinazione, che offrono un dispositivo di storage pronto all'uso per software di backup esterni come Veeam. Solo un dispositivo di destinazione progettato appositamente per il backup S3 e pronto all'uso offre una resilienza dei dati Zero Trust, separando correttamente software e storage, e consentendo test di sicurezza indipendenti.

Immutabilità assoluta: la difesa migliore contro il ransomware

Se non riesci a spuntare tutte le voci, i tuoi backup potrebbero essere vulnerabili agli attacchi ransomware. Immutabilità assoluta significa zero accesso ad azioni distruttive. Nessuno, nemmeno l'amministratore con i privilegi più elevati o un aggressore con accesso allo storage di backup, può alterare o eliminare i dati.

Per raggiungere **l'immutabilità assoluta** attraverso l'accesso zero, è necessario seguire **tre principi fondamentali:**

1. **Storage a oggetti S3:** uno standard aperto e completamente documentato, con immutabilità nativa integrata, che consente test di penetrazione e verifica indipendenti.
2. **Immutabilità immediata:** i dati di backup devono essere immutabili dal momento stesso in cui vengono scritti.
3. **Dispositivo di storage di destinazione:** un dispositivo di storage di destinazione dedicato separa lo storage dal software di backup e rimuove i rischi associati alla gestione fai-da-te dello storage di backup durante le operazioni.

Scarica il nostro white paper e scopri perché **l'immutabilità assoluta** è la resilienza definitiva contro il ransomware.

Scarica il nostro white paper ↗

Informazioni su Object First

Object First offre uno storage di backup sicuro, semplice e potente, progettato appositamente per Veeam, con immutabilità assoluta. Grazie alla difesa definitiva contro il ransomware, tu e la tua organizzazione diventate veramente resilienti.

Richiedi una Demo ↗