veeam Ready Repository

open-e JovianVHR

DEIN IMMUTABLE BACKUP IST NICHT SO UNVERÄNDERLICH, WIE DU DENKST.

Aufzeigen des Single Point of Failure in Standard-Linux-Hardened-Repositories und wie man ihn beseitigt.

Ein technisches Briefing für IT-Architekten, Administratoren und CIOs, die für die Datensicherheit und Resilienz im Unternehmen verantwortlich sind.

www.open-e.com

Die Ransomware-Bedrohung entwickelt sich weiter. **Ist Ihre Backup-Strategie bereit?**

Seit langem gilt **Daten-Unveränderlichkeit (Data Immutability)** als Goldstandard zum Schutz vor Ransomware und versehentlicher Datenlöschung. Doch das Vertrauen auf nur **eine einzige Schutzschicht** – etwa ein **XFS-Immutability-Flag**, wie es in derLinux-Hardened-Repository-Funktion verwendet wird, schafft eine **kritische Schwachstelle**. Diese nennen wir den **Single Point of Failure (SPOF)**.

Die Schwachstelle einstufiger Immutability

Stellen Sie sich ein digitales Schloss für Ihre Daten vor: Solange der Schlüssel vorhanden ist, sind Ihre Dateien vor Veränderung oder Löschung geschützt. Doch was passiert, wenn genau dieser Schlüssel kompromittiert wird?

Lösungen, die auf einem **Immutability-Flag** basieren, sind verwundbar. Dieses Flag kann versehentlich, durch einen böswilligen Akteur oder durch einen technischen Fehler entfernt werden. Sobald es verschwindet, sind Ihre Daten vollständig ungeschützt und eine Wiederherstellung nach einem Angriff ist unmöglich. Das ist das Wesen des **SPOF**: ein einzelner Fehlerpunkt, der, sobald ausgenutzt, die gesamte Sicherheitskette zum Einsturz bringt.

Die Standard-XFS-Unveränderlichkeit bietet zwar eine starke erste Verteidigungslinie, ist jedoch nicht unverwundbar gegen kompromittierte Superuser. Fortgeschrittene Bedrohungen, böswillige Insider oder versehentliche administrative Fehler können dennoch zu katastrophalem Datenverlust führen.

Die ernüchternde Realität

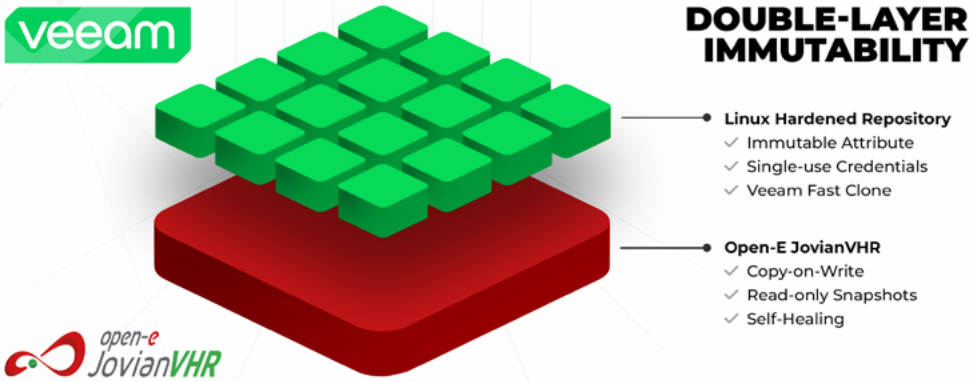
- **59%** aller Unternehmen wurden im letzten Jahr Opfer eines Ransomware-Angriffs. (Quelle: 2024 Sophos „State of Ransomware“-Report)
- **2.73Mio** Mio. USD durchschnittliche Gesamtkosten (ohne Lösegeldzahlungen).

Ein **Single Point of Failure** ist keine Option mehr. Sie benötigen eine **zweite, unabhängige Verteidigungsschicht**, die direkt im Kern Ihrer Datenspeicherung integriert ist.

Das Paradox des Root-Zugriffs

Wenn ein Angreifer Root-Zugriff auf den Linux-Hardened-Repository-Server erhält oder ein Insider über gültige Zugangsdaten verfügt, hält er den sprichwörtlichen „Schlüssel zum Königreich“. Mit Root-Rechten kann die XFS-basierte Immutability, auf die sich das Hardened Repository stützt, systematisch außer Kraft gesetzt werden. Dieser Angriffsvektor umgeht alle Schutzmechanismen innerhalb des Linux-Hardened-Repositories, weil er direkt auf der Betriebssystemebene ansetzt. Das Werkzeug, das eigentlich für Wartungszwecke gedacht ist, wird zur Waffe gegen die eigene Datensicherheit.

Die zentrale Herausforderung ist klar:
Echte Daten-Unveränderlichkeit darf nicht einer einzigen Sicherheitsschicht anvertraut werden,die vom selben System deaktiviert werden kann, das sie eigentlich schützen soll.



Ein Ansatz mit doppellagiger Immutability

Bei Open-E sind wir überzeugt, dass Sicherheit mehr als nur ein Schloss braucht. Unsere Lösung bietet ein **zweistufiges Immutability-System.**

- **Primäre Schicht:** Basierend auf dem **Linux Hardened Repository** von Veeam®, das die XFS-Immutability-Flag-Funktion und Single-Use-Credentials unterstützt.
- **Sekundäre Schicht:** Eine ultimative Verteidigungsebene, die auf **ZFS-Read-only-Snapshots** basiert.

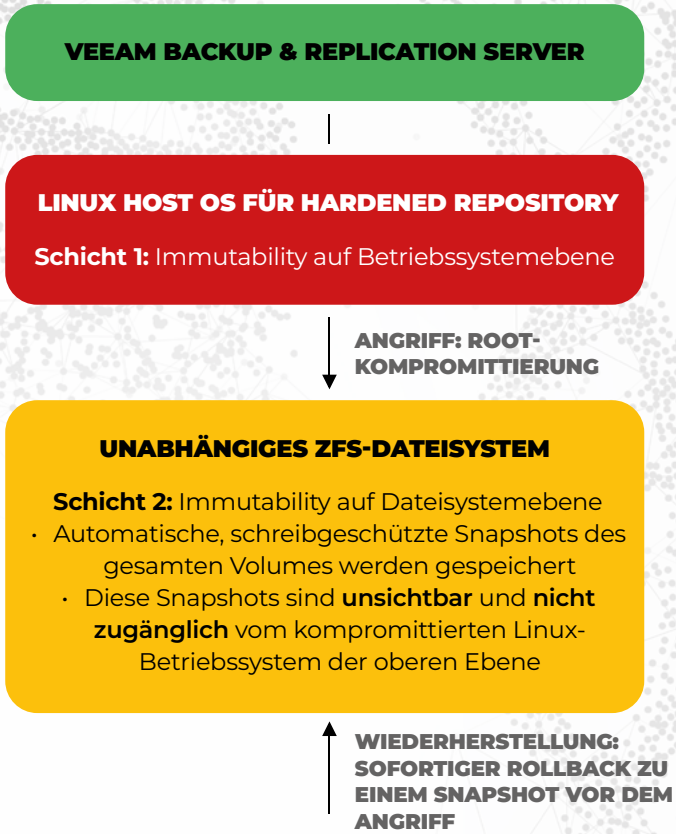
Selbst wenn ein Angreifer die erste Schicht umgeht, bleibt die zweite intakt. Die ZFS-Snapshots erzeugen ein dauerhaftes, manipulationssicheres Protokoll Ihrer Daten zu verschiedenen Zeitpunkten. Das bedeutet, Sie können jederzeit auf einen sauberen Zustand vor dem Angriff zurücksetzen und so die Bedrohung neutralisieren, bevor sie Schaden anrichtet.

Mit dem **zweistufigen Immutability-Schutz** von Open-E sind Sie nicht nur geschützt, sondern widerstandsfähig. Unsere Lösung stellt sicher, dass Sie selbst dann einen Backup-Plan haben, wenn eine Verteidigung versagt.

Architektur für Resilienz: Der Fall für doppellagige Immutability

Um die Schwachstelle durch Root-Kompromittierung zu beseitigen, muss der Datenschutz über das Betriebssystem hinausgehen und auf einer grundlegenderen Ebene durchgesetzt werden: dem **Dateisystem**. Dadurch entstehen zwei unabhängige, nicht miteinander kommunizierende Sicherheitsschichten.

veeam Ready Repository



Schicht 1: Die Betriebssystemebene
Dies ist das Linux-Hardened-Repository-Modell, das im Veeam Backup & Replication System verwendet wird. Es schützt wirksam vor unbefugten Änderungen durch nicht privilegierte Benutzer und den Veeam Repository Service selbst. Diese Schicht bildet die entscheidende erste Verteidigungslinie gegen Angriffe auf Anwendungsebene.

- **Mechanismus:** XFS-Dateisystem mit Immutability-Flag
- **Steuerung:** Verwaltet durch Veeam Backup & Replication über Single-Use-Credentials
- **Schwäche:** Kann durch jeden Benutzer mit erweiterten Zugriffsrechten (typischerweise Root) außer Kraft gesetzt werden

Schicht 2: Die Dateisystemebene (Der ZFS-Vorteil)
Dies ist ein logisch isoliertes Schutzsystem. Durch den Einsatz eines fortschrittlichen Dateisystems wie **ZFS** lässt sich eine Historie der Daten erstellen, die unabhängig vom aktiven Betriebssystem existiert.

- **Mechanismus:** Atomare Copy-on-Write-Snapshots (CoW), schreibgeschützt. Ein Snapshot ist keine Kopie, sondern ein Satz von Verweisen auf Datenblöcke, die zu einem bestimmten Zeitpunkt eingefroren sind.
- **Steuerung:** Verwaltet durch ein separates, darunterliegendes Datenspeichersystem mit eigenen Zugangsdaten und Aufbewahrungsrichtlinien, vollständig isoliert vom Linux Hardened Repository.
- **Stärke:** Selbst wenn ein Angreifer Root-Zugriff auf das Repository erhält und alle Dateien löscht, werden nur Verweise aus dem Dateisystem entfernt. Die eigentlichen Datenblöcke bleiben durch die unabhängigen Snapshots erhalten und sind sofort wiederherstellbar.

Diese Architektur mit doppellagiger Immutability verwandelt das Repository von einer einfachen Sicherheitsbox in einen digitalen Tresor mit Zeitsperre.

Open-E JovianVHR: Die kosteneffiziente, leistungsstarke und wirklich unveränderliche Basis für Ihr Hardened Repository

Entwickelt, um Ransomware, Insider-Bedrohungen und Datenkorruption zu verhindern.

Nachdem die Herausforderungen definiert sind, stellen wir nun die speziell entwickelte Lösung vor. Open-E JovianVHR ist ein Software-Defined-Storage-System, das gezielt dafür konzipiert wurde, die ideale Grundlage für ein Hardened Repository in Verbindung mit Veeam zu schaffen. Es adressiert die zentralen technischen Herausforderungen von Immutability, Integrität und Performance.

Wie Open-E JovianVHR diese Herausforderungen löst

- **Echte doppellagige Immutability**
  Implementiert die ZFS-Dateisystem-Ebene, die automatisierte, unveränderliche und betriebssystemunabhängige Snapshots Ihrer Backup-Daten erstellt. Dies ist Ihre Verteidigung gegen Root-Kompromittierungen und Insider-Bedrohungen.
- **Garantierte Datenintegrität**
  ZFS bietet End-to-End-Checksummen für jeden Datenblock. Es überprüft kontinuierlich die Datenintegrität und repariert in einem redundanten Array (RAID-Z) automatisch beschädigte Blöcke, sodass Ihre Backups stets gültig bleiben.
- **Performance auf Enterprise-Niveau**
  Durch den Einsatz von ZFS-Caching (ARC), Inline-Kompression (LZ4/Zstd) und Unterstützung für Hochgeschwindigkeits-Hardware erreicht Open-E JovianVHR Datenraten im Multi-GB/s-Bereich. Das verkürzt Backup-Fenster erheblich und beschleunigt Veeam Instant VM Recovery®.
- **Niedriger TCO und kein Vendor Lock-In**
  Als Software-Defined-Storage-Lösung lässt sich Open-E JovianVHR auf beliebiger Standard-Hardware einsetzen. Ein einfaches, planbares Lizenzmodell ohne Gebühren pro Terabyte reduziert die Total Cost of Ownership (TCO) deutlich im Vergleich zu proprietären Appliances.

Über Immutability hinaus: Die grundlegenden Anforderungen an ein Backup-Ziel

Ein modernes Backup-Repository muss mehr leisten als nur unveränderlich zu sein. Es muss Datenintegrität garantieren und Performance bieten, um aggressive RTO-/RPO-Ziele zu erfüllen.

- **Die Bedrohung durch stille Korruption:** „Bit Rot“ ist ein reales Phänomen: Auf Speichermedien entstehen im Laufe der Zeit unbemerkte Datenfehler. Standard-Dateisysteme erkennen diese häufig nicht, was zu beschädigten Backup-Dateien führen kann, die erst bei einer Wiederherstellung auffallen.
- **Der Performance-Engpass:** Langsame Speicherlösungen können mit modernen Backup-Anforderungen nicht Schritt halten. Bei einer Wiederherstellung kann das zu verlängerten Ausfallzeiten führen, die von Minuten bis zu Stunden reichen und den Geschäftsbetrieb direkt beeinträchtigen.
- **Optimierte Gesamtbetriebskosten (TCO):** Durch den Einsatz handelsüblicher Hardware und Standard-Server ohne proprietäre Abhängigkeiten bleibt Open-E JovianVHR flexibel und kosteneffizient. Auch die Preisgestaltung ist bewusst einfach gehalten – Sie zahlen nur den gewünschten Support-Plan.

Open-E JovianVHR: Entwickelt für Enterprise-Effizienz

Ein Immutable Backup ist nutzlos, wenn es zu langsam ist, um Ihre RTO-Vorgaben zu erfüllen, oder zu teuer in der Umsetzung. Open-E JovianVHR basiert auf dem leistungsstarken ZFS-Dateisystem, das außergewöhnliche Geschwindigkeit und einen deutlich niedrigeren TCO bietet.

Hör auf, dir Sorgen um deine Backups zu machen

Erhalte Backup Storage in Enterprise-Qualität – sicher, zuverlässig und budgetfreundlich.

Open-E JovianVHR ist eine auf **ZFS** und Linux basierende software-definierte Storage-Lösung, die entwickelt wurde, um den Wert von **Hardened Repository**-Implementierungen zu maximieren.

Mit Fokus auf **Security** und **Data Integrity** ist es die ideale Basis für dein **Hardened Repository** von **Veeam**.

Bereit, dich selbst zu überzeugen?

Lade unsere kostenlose **60-Tage-Testversion** herunter und entdecke, wie einfach und sicher deine Backup-Strategie sein kann.

Keine Kreditkarte erforderlich.

open-e

Gegründet 1998, ist Open-E ein etablierter Entwickler von IP-basierter Storage-Management-Software.
Unser Flaggschiff-Produkt **Open-E JovianDSS** ist eine leistungsstarke, umfassende und preisgekrönte Data-Storage-Applikation, bekannt für hervorragende Kompatibilität, Benutzerfreundlichkeit und Stabilität. Mit über **40.000 Installationen weltweit** ist es unangefochtener Marktführer in Preis-Leistung.
Auf Basis dieser Expertise haben wir **Open-E JovianVHR** entwickelt – eine software-definierte Data-Storage-Lösung, die speziell dafür konzipiert ist, als unveränderbares Datenspeicherziel (immutable storage target) für ein **Hardened Repository** von **Veeam** zu dienen. Dank unserer Reputation für geschäftliche Zuverlässigkeit und Innovationskraft ist Open-E heute der bevorzugte Technologiepartner führender IT-Unternehmen.

+41,000 Software-Implementierungen

+25 Jahre Erfahrung

+120 Länder weltweit

+800 zertifizierte Engineers und Sales-Profis

Open-E, Inc.
+1 (678) 666 2880 (US) | +49 (89) 800 777 0 (Europe)
info@open-e.com