veeam Ready Repository

open-e JovianVHR

YOUR IMMUTABLE BACKUP ISN'T AS IMMUTABLE AS YOU THINK

Exposing the Single Point of Failure in Standard Linux Hardened Repositories and How to Eliminate It

A technical brief for IT architects, administrators, and CIOs responsible for enterprise data resilience

www.open-e.com

The Ransomware Threat Evolves. **How About Your Backup Strategy?**

For a long time, data immutability has been the gold standard for protecting against ransomware and accidental data deletion. However, relying on a single layer of protection, like an XFS immutability flag provided by the Linux Hardened Repository feature, creates a critical weakness. We call this the Single Point of Failure (SPOF).

The Flaw in Single-Layer Immutability

Imagine a digital lock on your data. As long as the key is in place, your files are safe from being altered or deleted. But what happens if that single key is compromised?

Solutions relying on an immutability flag are vulnerable. The flag can be removed by accident, a malicious actor, or a technical glitch. Once it's gone, your data is completely exposed, leaving you with no way to recover from an attack. This is the essence of the SPOF: a single point of failure that, once exploited, brings down the entire security chain.

Standard XFS-level immutability is a powerful first line of defense, but it's not invincible against a compromised superuser. Advanced threats, malicious insiders, or accidental administrative errors can still lead to catastrophic data loss.

The Sobering Reality:

- **59%** of organizations were attacked by ransomware in the last year. (Source: 2024 Sophos „State of Ransomware" Report)
- **$2.73M overall** recovery costs (excluding any ransom payment)

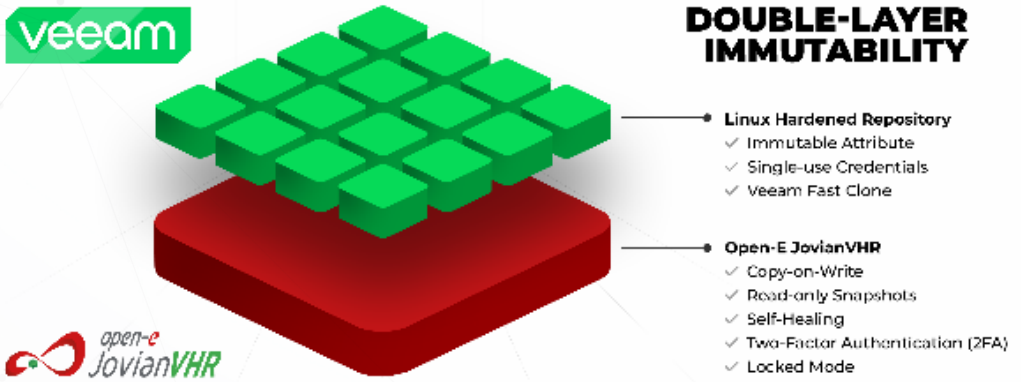
A single point of failure is no longer an option. You need a second, independent layer of defense built into the core of your data storage.

The Paradox of Root Access

An attacker who gains root access to the Linux hardened repository server or a malicious insider with legitimate credentials holds the „single key to the kingdom." With root privileges, the XFS-level immutability that the hardened repository relies on can be systematically dismantled.

This attack vector bypasses the protection mechanisms within Linux Hardened Repository because it occurs directly on the repository's operating system. The very tool designed for system maintenance becomes the weapon for its destruction.

The core challenge is clear: True data immutability cannot be entrusted to a security layer that can be disabled by the same system it is designed to protect.



A Double-Layer Immutability Approach

At Open-E, we believe in building security with more than one lock. Our solution provides a double-layer immutability system.

- **Primary Layer:** based on the Linux Hardened Repository provided by Veeam® that supports the XFS immutability flag feature and single-use credentials.
- **Secondary Layer:** An ultimate line of defence powered by ZFS read-only snapshots.

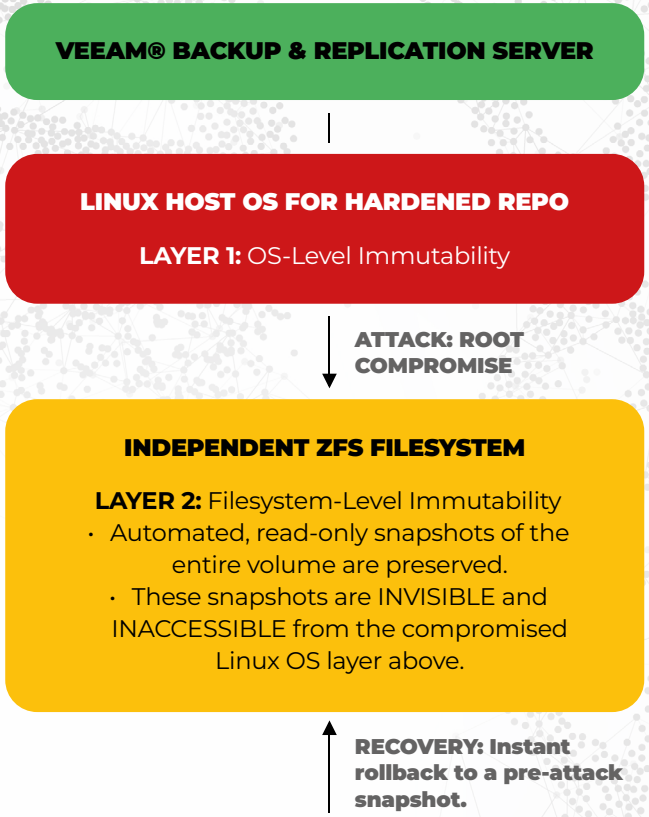
Even if an attacker bypasses the first layer, the second one remains intact. The ZFS snapshots create a permanent, tamper-proof record of your data at various points in time. This means you can instantly roll back to a clean, pre-attack state, neutralizing the threat before it causes lasting damage.

With Open-E JovianVHR's double-layer immutability protection, you're not just protected. You're resilient. Our solution ensures that even if one defense fails, you'll always have a backup plan.

Architecting for Resilience: The Case for Double-Layer Immutability

To solve the root compromise vulnerability, data protection must move beyond the operating system and be enforced at a more fundamental level: the filesystem. This creates two independent, non-communicating layers of security.

veeam Ready Repository



Layer 1: The Operating System Layer

This is the Linux Hardened Repository model used by the Veeam Backup & Replication system. It's effective at preventing unauthorized changes from non-privileged users and from the Veeam repository console itself. It's a crucial first line of defense against application-level attacks.

- **Mechanism:** XFS filesystem immutability flag.
- **Control:** Managed by Veeam Backup & Replication via single-use credentials.
- **Weakness:** Can be undone by any user with high-level access capability (typically, root).

Layer 2: The Filesystem Layer (The ZFS Advantage)

This is a logically air-gapped protection scheme. By using an advanced filesystem like ZFS, we can create a history of the data that exists independently of the live OS.

- **Mechanism:** Atomic, copy-on-write (CoW), read-only snapshots. A snapshot isn't a copy; it's a set of pointers to data blocks that are frozen in time.
- **Control:** Managed by a separate, underlying data storage system with its own credentials and retention policy, completely isolated from the Linux Hardened Repository.
- **Strength:** Even if an attacker gains root on the repository OS and deletes every file, they are only removing pointers from the live filesystem. The data blocks themselves, referenced by the independent snapshots, remain untouched and instantly recoverable.

This double-layer immutability architecture transforms the repository from a single-lock box into a digital vault with a time lock.

Open-E JovianVHR: The Cost-Effective, High-Performance, and Truly Immutable Foundation for Your Hardened Repository.

Engineered to defeat ransomware, insider threats, and data corruption.

Having defined the challenges, we can now introduce the purpose-built solution. Open-E JovianVHR is a Software-Defined Storage system designed specifically to create the ultimate foundation for a Hardened Repository from Veeam, addressing the core technical challenges of immutability, integrity, and performance.

How Open-E JovianVHR Solves the Challenges:

- **True, Double-layer Immutability**
  It implements the ZFS Filesystem Layer, creating automated, unchangeable, and OS-independent snapshots of your backup data. This is your defense against root compromise and insider threats.
- **Guaranteed Data Integrity**
  ZFS provides end-to-end checksumming on every data block. It constantly verifies data integrity and, in a redundant array (RAID-Z), will automatically self-heal corrupt blocks, ensuring your backups are always valid.
- **Enterprise-Grade Security**
  It provides advanced security by using two-factor authentication (2FA) to stop unauthorized remote access to the management interface. Additionally, its locked mode protects critical information by requiring physical access to the server for any administrative tasks that involve changing or deleting data.
- **Lower TCO & No Vendor Lock-In**
  As a Software-Defined Storage solution, you deploy Open-E JovianVHR on the commodity hardware of your choice. A simple, predictable licensing model without per-terabyte fees dramatically lowers the TCO compared to proprietary appliances.

Beyond Immutability: The Foundational Requirements for a Backup Target

A modern backup repository must do more than just be immutable. It must guarantee data integrity and deliver performance that meets aggressive RTOs/RPOs.

- **The Threat of Silent Corruption:** “Bit rot” is a real phenomenon where data on data storage media degrades over time. Standard filesystems may not detect this, leading to a corrupt backup file that is only discovered during a critical restore attempt.
- **The Performance Bottleneck:** Slow data storage can’t keep up with modern backup demands, leading to missed backup windows. During a recovery, slow storage can extend downtime from minutes to hours, directly impacting the business.
- **Optimised Total Cost of Ownership (TCO):** Use commodity hardware and deploy on the industry-standard servers with no proprietary hardware lock-in. Open-E JovianVHR’s pricing is also designed to be straightforward, so you only pay for the support plan of your choice.

Open-E JovianVHR: Engineered for Enterprise Efficiency

An immutable backup is useless if it’s too slow to meet your RTOs or too expensive to deploy. Open-E JovianVHR is built on the high-performance ZFS filesystem, delivering exceptional speed and a dramatically lower TCO.

Stop worrying about your backups

DOWNLOAD NOW!

Get enterprise-grade backup storage that's secure, reliable, and easy on your budget.

Open-E JovianVHR is a ZFS- and Linux-based software-defined storage solution designed to maximize the value of Hardened Repository implementations.

With a focus on **security** and **data integrity**, it's the perfect data storage foundation for your Hardened Repository from Veeam.

Ready to see for yourself?

Download our free, **60-day trial** and discover how simple and secure your backup strategy can be.

No credit card required.

open-e

Founded in 1998, Open-E is a well-established developer of IP-based storage management software. Our flagship product, **Open-E JovianDSS**, is a robust, comprehensive, and award-winning data storage application known for its excellent compatibility, ease of use, and stability. It's an undisputed leader in price-performance with over 40,000 installations worldwide.

Building on this expertise, we've introduced **Open-E JovianVHR**, a software-defined data storage solution specifically designed to act as the immutable data storage target for a Hardened Repository from Veeam. With a reputation for business reliability and a commitment to innovation, Open-E has become the technology partner of choice for industry-leading IT companies.

+41,000 software implementations

+28 years of experience

+120 countries worldwide

+800 certified engineers and sales professionals

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