



# Security Transformed. Resilience Rehearsed. Identity Protected.



## VEEAM DATA PLATFORM V13.1

**Veeam Backup & Replication v13.1** addresses three enterprise-scale challenges with precision: hypervisor migration at pace, an identity-centric threat environment where a single compromised identity system can halt an entire organization, and sprawling hybrid estates. For federal agencies, v13.1 delivers post-quantum cryptography aligned with EO 14412, wizard-driven AD Forest Recovery, a DISA STIG-hardened appliance, and critical CVE remediations — everything needed to protect, prove, and recover mission-critical data.

**70+** New Features & Enhancements  
**13** Supported Hypervisors  
**5** New Hypervisor Platforms

## VDP V13.1 — FEDERAL MISSION CAPABILITIES

### SM Tape & Air-Gap

- LTO-10 drive & media support with catalog improvements
- Tape = cleanest offline copy for 3-2-1-1-0 rule
- NARA 36 CFR 1236 compliant long-term retention
- Air-gap for classified & sensitive workloads

### OpenShift Virtualization Engine (OVE)

- Agentless hostbased VM backup; no ingest agents required
- Managed in the same VBR console. Cross platform recovery: OVE migration path
- Veeam Kasten adds container + VM coverage in airgapped clusters
- Universal Hypervisor API Plug in

### Security & Hardening

- Post-quantum crypto (ML-KEM, EO 14412 compliant)
- CVSS 9.9 + 9.1 CVEs fully patched in v13.1
- VSA: DISA STIG pre-hardened, FIPS global mode
- Single-port transport; MFA on all sensitive ops



### Multi-Hypervisor Future

13 platforms total. v13.1 adds Citrix XenServer, XCP-ng, Sangfor aSV, Platform9, and VergeOS. New Universal Hypervisor API (UHAPI) opens a vendor-certified path for additional platforms. Single universal worker image is FIPS and DISA STIG compliant across all hypervisors.



### Guided AD Forest Recovery

Wizard covers single-domain, multi-domain, and multi-tree AD topologies. Automated FSMO seizure, krbtgt reset, DC rejoin, and replication validation. Entra ID gains persistent object relationship reconstruction and expanded BitLocker recovery key coverage.



### Post-Quantum Cryptography

ML-KEM (FIPS 203/204/205) hybrid model: PQC for handshake and key exchange, FIPS-certified AES for data encryption. Enables on existing deployments without data migration or infrastructure changes. When FIPS-only mode is on, PQC disables automatically for full FIPS adherence.



### MFA Enforcement & Audit Trail

Users and Roles changes require MFA confirmation. Encryption password changes logged in session history for key rotation audit trail. FIPS compliance mode enforced globally across system and application components. Supports Zero Trust architecture for backup infrastructure.



### Faster Linux File-Level Restore

Significant speed improvements via proxy assignment and transport mode refinements. Critical for physical server recovery in air-gapped federal environments where Linux agents protect mission workloads and RTO targets are measured in minutes, not hours.



### LTO-10 Tape & Air-Gap Compliance

LTO-10 drive and media support with catalog and performance improvements. Continues federal air-gap and offline copy compliance — the offline tier of the 3-2-1-1-0 rule. Critical for agencies maintaining NARA-compliant long-term offline retention schedules.



### SureBackup & SIEM Audit Trail

Expanded application testing scripts reduce false failures. Trackable restore events via syslog and Incident API provide the audit-ready verification cadence required for RMF and FISMA compliance documentation. Improved Veeam ONE dashboard reporting.



### PostgreSQL Default Database

PostgreSQL is the default VBR backend — SQL Server is on sunset roadmap. v12.x to v13.1 in-place upgrade supported and documented. Single-port secure transport simplifies firewall rules in segmented federal networks and SCIF architectures.



### Immutability & Object Storage

Expanded S3-compatible WORM with on-prem immutability — no cloud dependency. Supports NARA records management and ransomware resilience on-premises. BLAKE3 hashing improves dedup and verification throughput. Tighter capacity-tier integration for long-term retention.



### VSA Observability & HA

Prometheus-compatible metrics via Node Exporter for integration with existing monitoring stacks. Syslog forwarding for SIEM and compliance audit trails. Cross-subnet HA clustering with data lag and version observability. Private fix synchronization between HA nodes.

## ABOUT VEEAM SOFTWARE

Veeam is the Data and AI Trust Company and the market leader in both data resilience and data security posture management, Veeam is built for the convergence of identity, data, security, and AI risk. Headquartered in Seattle, Veeam protects over 550,000 customers worldwide. Learn more at [www.veeam.com](https://www.veeam.com) or follow Veeam on LinkedIn [@veeam-software](https://www.linkedin.com/company/veeam) and X [@veeam](https://twitter.com/veeam).

➤ If you would like to learn more or connect, please [request a meeting](#).