

# ZeroVault

Fully Managed, S3-Compatible Cloud Storage Service for Veeam

*“Zero compromise.” — An attacker can never find a copy they can’t delete.*

|          |                                                                       |
|----------|-----------------------------------------------------------------------|
| Service  | ZeroVault — Cloud-Based Immutable Object Storage Service              |
| Focus    | Fully managed, immutable cloud storage for Veeam Backup & Replication |
| Version  | 1.0                                                                   |
| Date     | June 2026                                                             |
| Coverage | BDDK · SPK · DORA · KVKK · GDPR · ISO 27001 · NIST                    |
| Provider | BackupSec                                                             |

## 1. What is ZeroVault?

ZeroVault is a fully managed cloud storage service purpose-built for Veeam Backup & Replication environments — S3-compatible, immutable, and logically air-gapped. There's no hardware to buy, no data center space to allocate, and no storage infrastructure to maintain; ZeroVault is delivered as a cloud service and provisioned in minutes. Even if an attacker compromises the backup infrastructure, gains domain admin rights, and accesses the Veeam config database — backup copies in ZeroVault can be neither deleted nor encrypted before the retention period expires. ZeroVault is the cloud storage layer of the BackupSec family, complementing ZeroMON monitoring, ZeroTAM advisory, and ZeroPEN penetration testing.

**Why immutable storage?** The common thread across modern ransomware attacks is finding and destroying backups before encrypting production. A writable repository is just a target for an attacker with enough privilege. ZeroVault makes the privilege itself irrelevant: the delete command runs, but the data stays put.

### Four layers, zero compromise

ZeroVault works alongside the rest of the BackupSec family:

| Service          | Role                                                                                           |
|------------------|------------------------------------------------------------------------------------------------|
| ZeroMON          | Observability platform — real-time monitoring and security signals                             |
| ZeroTAM          | Expert advisory — architecture, capacity, strategy and crisis support                          |
| ZeroPEN          | Penetration test & recovery proof — tests backups the way an attacker would                    |
| <b>ZeroVault</b> | <b>Cloud storage service — a last copy that cannot be deleted or encrypted (this document)</b> |

### Who is it for?

- Veeam users who want to fully implement the immutable cloud copy in the 3-2-1-1-0 rule
- Organizations that want immutable storage as a service, without managing hardware
- Organizations securing the last line of defense against ransomware
- Organizations needing an immutable cloud archive for regulatory retention periods
- IT teams looking for cost-predictable, egress-free cloud storage
- Organizations with BDDK / SPK / DORA / KVKK / GDPR obligations

## 2. Cloud Architecture & Technical Specifications

ZeroVault's technical specifications as a cloud storage service:

| Area                              | Specification                                                                                                    |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Deployment Model</b>           | Fully managed cloud storage service — no hardware to buy, install, or maintain; provisioned in minutes           |
| <b>Immutability</b>               | Object Lock (WORM), governance & compliance mode, configurable retention period (days/years), legal hold support |
| <b>Architectural Isolation</b>    | Logical air-gap from the production network, separate credentials/IAM, write-once-read-many enforcement          |
| <b>Protocol &amp; Integration</b> | Amazon S3 API compatible; native integration with Veeam Backup & Replication and Veeam Data Platform             |
| <b>Veeam Repository Mode</b>      | Usable as a direct object storage repository or as a SOBR capacity/performance tier                              |
| <b>Data Durability</b>            | Eleven nines (99.999999999%) durability, replicated across multiple availability zones                           |
| <b>Geographic Coverage</b>        | Multi-region cloud deployment options — choose region for data residency needs                                   |
| <b>Encryption</b>                 | AES-256 encryption in transit and at rest                                                                        |
| <b>Cost Predictability</b>        | Predictable cloud storage economics with no hidden egress or API-call fees                                       |
| <b>Compliance Posture</b>         | Cloud infrastructure aligned with HIPAA, GDPR, PCI-DSS and SOC 2 Type II requirements                            |
| <b>Management</b>                 | Centralized web console, BackupSec-branded access, API-driven provisioning — no servers to manage                |

### 3. Veeam Integration

ZeroVault can be used with Veeam Backup & Replication in two ways:

- 1 Direct Object Storage Repository — backup jobs write directly to ZeroVault.
- 2 SOBR Capacity/Performance Tier — used as the immutable tier to which older restore points are automatically offloaded in a Scale-Out Backup Repository configuration.

**Logical air-gap:** ZeroVault access credentials are managed separately from the Veeam management plane and Active Directory. Even if AD is compromised, there is no direct destructive path to ZeroVault.

### 4. Use Cases

| Scenario                        | Description                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Last-Copy Resilience            | The last line of defense satisfying the “1” (immutable) and “0” (verified restore) components of the 3-2-1-1-0 rule |
| Ransomware-Resilient Repository | A backup copy that cannot be deleted or encrypted even if an attacker gains domain admin rights                     |
| Compliance Archive              | Immutable long-term archive that satisfies regulatory retention periods                                             |
| Disaster Recovery Cloud Tier    | Cost-predictable storage for an off-site / cloud DR copy                                                            |

## 5. Regulatory Coverage

| Regulation       | Requirements ZeroVault Supports                                            |
|------------------|----------------------------------------------------------------------------|
| BDDK             | Art.45 backup, BT.31 ransomware controls — an immutable last copy          |
| SPK III-35.1     | Data retention periods, immutable archive for business continuity          |
| DORA (EU)        | Art.11-12 backup policy — immutable, air-gapped copy requirement           |
| KVKK             | Art.12 technical measures — immutable & encrypted storage of personal data |
| GDPR (EU)        | Art.32 security measures — encryption and integrity protection             |
| ISO 27001 / NIST | A.12.3 backup, A.8.3 media handling, NIST SP 800-209 storage security      |

## 6. Next Step

**To get started:** BackupSec works with you to plan region, retention and access configuration for integrating ZeroVault into your existing Veeam environment as a repository or SOBR capacity tier.