

ZeroVault

面向 Veeam 的全托管、S3 兼容云存储服务

“零妥协。” — 攻击者永远找不到一份他们能够删除的副本。

服务	ZeroVault — 基于云的不可变对象存储服务
聚焦	面向 Veeam Backup & Replication 的全托管、不可变云存储
版本	1.0
日期	2026年6月
覆盖范围	BDDK · SPK · DORA · KVKK · GDPR · ISO 27001 · NIST
提供方	BackupSec

1. 什么是 ZeroVault?

ZeroVault 是一项专为 Veeam Backup & Replication 环境打造的全托管云存储服务 — S3 兼容、不可变且在逻辑上气隙隔离。无需购买硬件、无需分配数据中心空间、也无需维护存储基础设施；ZeroVault 以云服务方式交付，并可在几分钟内完成置备。即使攻击者攻陷了备份基础设施、获得了域管理员权限并访问了 Veeam 配置数据库 — 在保留期到期之前，ZeroVault 中的备份副本既无法被删除，也无法被加密。ZeroVault 是 BackupSec 家族的云存储层，与 ZeroMON 监控、ZeroTAM 咨询和 ZeroPEN 渗透测试互为补充。

为什么选择不可变存储？ 现代勒索软件攻击的共同点是：在加密生产环境之前先找到并摧毁备份。对于拥有足够权限的攻击者而言，可写的存储库只不过是一个攻击目标。ZeroVault 让权限本身变得无关紧要：删除命令照常执行，但数据岿然不动。

四层防护，零妥协

ZeroVault 与 BackupSec 家族的其余成员协同工作：

服务	角色
ZeroMON	可观测性平台 — 实时监控与安全信号
ZeroTAM	专家咨询 — 架构、容量、策略与危机支持
ZeroPEN	渗透测试 & 恢复验证 — 以攻击者的方式测试备份
ZeroVault	云存储服务 — 一份无法被删除或加密的最后副本（本文档）

适用于谁？

- 希望在 3-2-1-1-0 规则中完整落实不可变云副本的 Veeam 用户
- 希望以服务方式获得不可变存储、无需管理硬件的组织
- 为抵御勒索软件而巩固最后一道防线的组织
- 需要不可变云归档以满足法规保留期的组织
- 寻求成本可预测、无出口费用云存储的 IT 团队
- 负有 BDDK / SPK / DORA / KVKK / GDPR 合规义务的组织

2. 云架构 & 技术规格

ZeroVault 作为云存储服务的技术规格：

领域	规格
部署模型	全托管云存储服务 — 无需购买、安装或维护硬件；几分钟内完成置备
不可变性	Object Lock (WORM)、治理 & 合规模式、可配置的保留期（天/年）、法律保留支持
架构隔离	与生产网络的逻辑气隙隔离、独立的凭证/IAM、一次写入多次读取的强制执行
协议 & 集成	兼容 Amazon S3 API；与 Veeam Backup & Replication 和 Veeam Data Platform 原生集成
Veeam 存储库模式	可用作直接对象存储库，或用作 SOBR 容量/性能层
数据持久性	十一个九 (99.999999999%) 的持久性，跨多个可用区复制
地理覆盖	多区域云部署选项 — 根据数据驻留需求选择区域
加密	传输中和静态时均采用 AES-256 加密
成本可预测性	可预测的云存储成本，无隐藏的出口费用或 API 调用费用
合规态势	符合 HIPAA、GDPR、PCI-DSS 和 SOC 2 Type II 要求的云基础设施
管理	集中式 Web 控制台、BackupSec 品牌化访问、API 驱动的置备 — 无需管理服务器

3. Veeam 集成

ZeroVault 可通过两种方式与 Veeam Backup & Replication 配合使用：

- 1 直接对象存储库 — 备份作业直接写入 ZeroVault。
- 2 SOBR 容量/性能层 — 在 Scale-Out Backup Repository 配置中用作不可变层，较旧的恢复点会自动卸载到该层。

逻辑气隙隔离： ZeroVault 的访问凭证独立于 Veeam 管理平面和 Active Directory 进行管理。即使 AD 被攻陷，也不存在通往 ZeroVault 的直接破坏性路径。

4. 应用场景

场景	描述
最后副本韧性	满足 3-2-1-1-0 规则中“1”(不可变) 和“0”(经验证的恢复) 要素的最后一道防线
抗勒索软件存储库	即使攻击者获得域管理员权限也无法被删除或加密的备份副本
合规归档	满足法规保留期的不可变长期归档
灾难恢复云层	为异地 / 云 DR 副本提供成本可预测的存储

5. 法规覆盖

法规	ZeroVault 支持的要求
BDDK	Art.45 备份、BT.31 勒索软件控制 — 一份不可变的最后副本
SPK III-35.1	数据保留期，用于业务连续性的不可变归档
DORA (EU)	Art.11-12 备份策略 — 不可变、气隙隔离副本要求
KVKK	Art.12 技术措施 — 个人数据的不可变 & 加密存储
GDPR (EU)	Art.32 安全措施 — 加密和完整性保护
ISO 27001 / NIST	A.12.3 备份、A.8.3 介质处理、NIST SP 800-209 存储安全

6. 下一步

如何开始： BackupSec 将与您共同规划区域、保留期和访问配置，以将 ZeroVault 作为存储库或 SOBR 容量层集成到您现有的 Veeam 环境中。