

ZeroVault

Veeam을 위한 완전 관리형 S3 호환 클라우드 스토리지 서비스

“타협은 없다.” — 공격자는 자신이 삭제할 수 없는 사본을 결코 찾아낼 수 없습니다.

서비스	ZeroVault — 클라우드 기반 불변 오브젝트 스토리지 서비스
중점 영역	Veeam Backup & Replication을 위한 완전 관리형 불변 클라우드 스토리지
버전	1.0
날짜	2026년 6월
적용 범위	BDDK · SPK · DORA · KVKK · GDPR · ISO 27001 · NIST
제공자	BackupSec

1. ZeroVault란?

ZeroVault는 Veeam Backup & Replication 환경을 위해 특별히 설계된 완전 관리형 클라우드 스토리지 서비스로, S3 호환, 불변성, 논리적 에어갭을 제공합니다. 구매할 하드웨어도, 할당할 데이터센터 공간도, 유지 관리할 스토리지 인프라도 없습니다. ZeroVault는 클라우드 서비스로 제공되어 몇 분 만에 프로비저닝됩니다. 공격자가 백업 인프라를 장악하고 도메인 관리자 권한을 획득하며 Veeam 구성 데이터베이스에 접근하더라도 — ZeroVault의 백업 사본은 보존 기간이 만료되기 전에는 삭제하거나 암호화할 수 없습니다. ZeroVault는 BackupSec 제품군의 클라우드 스토리지 계층으로, ZeroMON 모니터링, ZeroTAM 자문, ZeroPEN 침투 테스트를 보완합니다.

왜 불변 스토리지인가? 현대 랜섬웨어 공격의 공통점은 프로덕션을 암호화하기 전에 백업을 찾아 파괴한다는 것입니다. 쓰기 가능한 리포지토리는 충분한 권한을 가진 공격자에게 그저 표적일 뿐입니다. ZeroVault는 그 권한 자체를 무의미하게 만듭니다. 삭제 명령은 실행되지만 데이터는 그대로 남아 있습니다.

4개 계층, 타협 없음

ZeroVault는 나머지 BackupSec 제품군과 함께 작동합니다:

서비스	역할
ZeroMON	업저버빌리티 플랫폼 — 실시간 모니터링 및 보안 신호
ZeroTAM	전문가 자문 — 아키텍처, 용량, 전략 및 위기 대응 지원
ZeroPEN	침투 테스트 & 복구 증명 — 공격자의 방식으로 백업을 테스트
ZeroVault	클라우드 스토리지 서비스 — 삭제하거나 암호화할 수 없는 마지막 사본 (본 문서)

누구를 위한 제품인가?

- 3-2-1-1-0 규칙의 불변 클라우드 사본을 완전히 구현하고자 하는 Veeam 사용자
- 하드웨어를 관리하지 않고 서비스형 불변 스토리지를 원하는 조직
- 랜섬웨어에 대한 최후의 방어선을 확보하려는 조직
- 규제 보존 기간을 위한 불변 클라우드 아카이브가 필요한 조직
- 비용 예측이 가능하고 이그레스 요금이 없는 클라우드 스토리지를 찾는 IT 팀
- BDDK / SPK / DORA / KVKK / GDPR 의무가 있는 조직

2. 클라우드 아키텍처 & 기술 사양

클라우드 스토리지 서비스로서 ZeroVault의 기술 사양:

영역	사양
배포 모델	완전 관리형 클라우드 스토리지 서비스 — 구매, 설치, 유지 관리할 하드웨어 없음; 몇 분 만에 프로비저닝
불변성	Object Lock (WORM), governance & compliance 모드, 구성 가능한 보존 기간(일/년), 리걸 홀드 지원
아키텍처적 격리	프로덕션 네트워크로부터의 논리적 에어갭, 별도의 자격 증명/IAM, write-once-read-many 적용
프로토콜 & 연동	Amazon S3 API 호환; Veeam Backup & Replication 및 Veeam Data Platform과의 네이티브 연동
Veeam 리포지토리 모드	직접 오브젝트 스토리지 리포지토리 또는 SOBR 용량/성능 계층으로 사용 가능
데이터 내구성	일레븐 나인(99.999999999%) 내구성, 여러 가용 영역에 걸쳐 복제
지리적 적용 범위	멀티 리전 클라우드 배포 옵션 — 데이터 레지던시 요구에 맞는 리전 선택
암호화	전송 중 및 저장 시 AES-256 암호화
비용 예측 가능성	숨겨진 이그레스 또는 API 호출 요금이 없는 예측 가능한 클라우드 스토리지 비용 구조
컴플라이언스 태세	HIPAA, GDPR, PCI-DSS 및 SOC 2 Type II 요구사항에 부합하는 클라우드 인프라
관리	중앙 집중식 웹 콘솔, BackupSec 브랜드 접근, API 기반 프로비저닝 — 관리할 서버 없음

3. Veeam 연동

ZeroVault는 Veeam Backup & Replication과 두 가지 방식으로 사용할 수 있습니다:

- 1 직접 오브젝트 스토리지 리포지토리 — 백업 작업이 ZeroVault에 직접 기록됩니다.
- 2 SOBR 용량/성능 계층 — Scale-Out Backup Repository 구성에서 오래된 복원 지점이 자동으로 오프로드되는 불변 계층으로 사용됩니다.

논리적 에어갭: ZeroVault 접근 자격 증명은 Veeam 관리 영역 및 Active Directory와 별도로 관리됩니다. AD가 침해되더라도 ZeroVault로 향하는 직접적인 파괴 경로는 없습니다.

4. 활용 사례

시나리오	설명
마지막 사본 복원력	3-2-1-1-0 규칙의 “1”(불변) 및 “0”(검증된 복구) 요소를 충족하는 최후의 방어선
랜섬웨어 복원력 리포지토리	공격자가 도메인 관리자 권한을 획득하더라도 삭제하거나 암호화할 수 없는 백업 사본
컴플라이언스 아카이브	규제 보존 기간을 충족하는 불변 장기 아카이브
재해 복구 클라우드 계층	오프사이트 / 클라우드 DR 사본을 위한 비용 예측 가능한 스토리지

5. 규제 적용 범위

규제	ZeroVault가 지원하는 요구사항
BDDK	Art.45 백업, BT.31 랜섬웨어 통제 — 불변의 마지막 사본
SPK III-35.1	데이터 보존 기간, 비즈니스 연속성을 위한 불변 아카이브
DORA (EU)	Art.11-12 백업 정책 — 불변, 에어갭 사본 요건
KVKK	Art.12 기술적 조치 — 개인정보의 불변 & 암호화 저장
GDPR (EU)	Art.32 보안 조치 — 암호화 및 무결성 보호
ISO 27001 / NIST	A.12.3 백업, A.8.3 미디어 취급, NIST SP 800-209 스토리지 보안

6. 다음 단계

시작하려면: BackupSec는 ZeroVault를 기존 Veeam 환경에 리포지토리 또는 SOBR 용량 계층으로 통합하기 위한 리전, 보존 및 접근 구성을 함께 계획합니다.