

ZeroVault

Veeam 向けのフルマネージド S3 互換クラウドストレージサービス

“妥協ゼロ。” — 攻撃者が、削除できないコピーを見つけ出すことは決してありません。

サービス	ZeroVault — クラウドベースのイミュータブルオブジェクトストレージサービス
重点領域	Veeam Backup & Replication 向けのフルマネージドなイミュータブルクラウドストレージ
バージョン	1.0
日付	2026年6月
対応範囲	BDDK・SPK・DORA・KVKK・GDPR・ISO 27001・NIST
プロバイダー	BackupSec

1. ZeroVault とは？

ZeroVault は、Veeam Backup & Replication 環境のために専用設計されたフルマネージドクラウドストレージサービスです — S3 互換、イミュータブル、そして論理的にエアギャップされています。購入すべきハードウェアも、割り当てるべきデータセンタースペースも、維持すべきストレージインフラもありません。ZeroVault はクラウドサービスとして提供され、数分でプロビジョニングされます。たとえ攻撃者がバックアップインフラを侵害し、ドメイン管理者権限を取得し、Veeam の構成データベースにアクセスしたとしても — ZeroVault 内のバックアップコピーは、保持期間が満了するまで削除も暗号化もできません。ZeroVault は BackupSec ファミリーのクラウドストレージレイヤーであり、ZeroMON のモニタリング、ZeroTAM のアドバイザリー、ZeroPEN のペネトレーションテストを補完します。

なぜイミュータブルストレージなのか？ 現代のランサムウェア攻撃に共通するのは、本番環境を暗号化する前にバックアップを見つけ出して破壊することです。書き込み可能なリポジトリは、十分な権限を持つ攻撃者にとって単なる標的にすぎません。ZeroVault は、その権限自体を無意味にします。削除コマンドは実行されても、データはそのまま残ります。

4つのレイヤー、妥協ゼロ

ZeroVault は BackupSec ファミリーの他の製品と連携して機能します：

サービス	役割
ZeroMON	オブザーバビリティプラットフォーム — リアルタイムモニタリングとセキュリティシグナル
ZeroTAM	エキスパートアドバイザリー — アーキテクチャ、キャパシティ、戦略、危機対応サポート
ZeroPEN	ペネトレーションテスト & リカバリ実証 — 攻撃者の視点でバックアップを検証
ZeroVault	クラウドストレージサービス — 削除も暗号化もできない最後のコピー（本書）

対象となるのは？

- 3-2-1-1-0 ルールにおけるイミュータブルなクラウドコピーを完全に実装したい Veeam ユーザー
- ハードウェアを管理することなく、サービスとしてのイミュータブルストレージを求める組織
- ランサムウェアに対する最後の防衛線を確保する組織
- 規制上の保持期間に対応するイミュータブルなクラウドアーカイブを必要とする組織
- コスト予測可能でイグレス料金のかからないクラウドストレージを求める IT チーム
- BDDK / SPK / DORA / KVKK / GDPR の義務を負う組織

2. クラウドアーキテクチャ & 技術仕様

クラウドストレージサービスとしての ZeroVault の技術仕様：

領域	仕様
デプロイモデル	フルマネージドクラウドストレージサービス — 購入・設置・維持すべきハードウェアなし。数分でプロビジョニング
イミュータビリティ	Object Lock (WORM)、ガバナンス & コンプライアンスモード、設定可能な保持期間（日/年）、リーガルホールド対応
アーキテクチャ上の分離	本番ネットワークからの論理的なエアギャップ、独立した認証情報/IAM、write-once-read-many の強制
プロトコル & 連携	Amazon S3 API 互換。Veeam Backup & Replication および Veeam Data Platform とのネイティブ連携
Veeam リポジトリモード	ダイレクトオブジェクトストレージリポジトリとして、または SOBR のキャパシティ/パフォーマンスティアとして利用可能
データ耐久性	イレブンナイン（99.999999999%）の耐久性、複数のアベイラビリティゾーンにレプリケート
地理的対応範囲	マルチリージョンのクラウド展開オプション — データレジデンシー要件に応じてリージョンを選択
暗号化	転送時および保管時の AES-256 暗号化
コストの予測可能性	隠れたイグレス料金や API 呼び出し料金のない、予測可能なクラウドストレージのコスト体系
コンプライアンス体制	HIPAA、GDPR、PCI-DSS、SOC 2 Type II の要件に準拠したクラウドインフラ
管理	一元化された Web コンソール、BackupSec ブランドのアクセス、API 駆動のプロビジョニング — 管理すべきサーバーなし

3. Veeam 連携

ZeroVault は、Veeam Backup & Replication と2つの方法で利用できます：

- 1 ダイレクトオブジェクトストレージリポジトリ — バックアップジョブが ZeroVault に直接書き込みます。
- 2 SOBR キャパシティ/パフォーマンスティア — Scale-Out Backup Repository 構成において、古いリストアポイントが自動的にオフロードされるイミュータブルティアとして使用されます。

論理的エアギャップ： ZeroVault のアクセス認証情報は、Veeam 管理プレーンおよび Active Directory とは別に管理されます。たとえ AD が侵害されても、ZeroVault への直接的な破壊経路は存在しません。

4. ユースケース

シナリオ	説明
ラストコピーのレジリエンス	3-2-1-1-0 ルールの“1”（イミュータブル）および“0”（検証済みリストア）の要素を満たす最後の防衛線
ランサムウェア耐性のあるリポジトリ	攻撃者がドメイン管理者権限を取得しても、削除も暗号化もできないバックアップコピー
コンプライアンスアーカイブ	規制上の保持期間を満たすイミュータブルな長期アーカイブ
ディザスタリカバリのクラウドティア	オフサイト / クラウド DR コピー向けの、コスト予測可能なストレージ

5. 規制対応範囲

規制	ZeroVault が対応する要件
BDDK	Art.45 バックアップ、BT.31 ランサムウェア対策 — イミュータブルな最後のコピー
SPK III-35.1	データ保持期間、事業継続性のためのイミュータブルアーカイブ
DORA (EU)	Art.11-12 バックアップポリシー — イミュータブルでエアギャップされたコピーの要件
KVKK	Art.12 技術的対策 — 個人データのイミュータブル & 暗号化ストレージ
GDPR (EU)	Art.32 セキュリティ対策 — 暗号化と完全性の保護
ISO 27001 / NIST	A.12.3 バックアップ、A.8.3 メディアの取り扱い、NIST SP 800-209 ストレージセキュリティ

6. 次のステップ

始めるには： BackupSec は、既存の Veeam 環境に ZeroVault をリポジトリまたは SOBR キャパシティティアとして統合するため、リージョン、保持期間、アクセス構成の計画をお客様と共に行います。