

ZeroVault

Veeam için Tümüyle Yönetilen, S3 Uyumlu Bulut Depolama Hizmeti

“Sıfır taviz.” — Bir saldırgan, silemeyeceği bir kopyayı asla bulamaz.

Hizmet	ZeroVault — Bulut Tabanlı Değişmez Nesne Depolama Hizmeti
Odak	Veeam Backup & Replication için tümüyle yönetilen, değişmez bulut depolama
Sürüm	1.0
Tarih	Haziran 2026
Kapsam	BDDK · SPK · DORA · KVKK · GDPR · ISO 27001 · NIST
Sağlayıcı	BackupSec

1. ZeroVault nedir?

ZeroVault, Veeam Backup & Replication ortamları için özel olarak geliştirilmiş, tümüyle yönetilen bir bulut depolama hizmetidir — S3 uyumlu, değişmez ve mantıksal olarak air-gap uygulanmış. Satın alınacak donanım, ayrılacak veri merkezi alanı ve bakımını üstleneceğiniz depolama altyapısı yoktur; ZeroVault bir bulut hizmeti olarak sunulur ve dakikalar içinde devreye alınır. Bir saldırgan backup altyapısını ele geçirirse, domain admin yetkileri elde etse ve Veeam yapılandırma veritabanına erişse bile — ZeroVault'taki backup kopyaları, saklama süresi dolmadan ne silinebilir ne de şifrelenebilir. ZeroVault, BackupSec ailesinin bulut depolama katmanıdır; ZeroMON izlemeyi, ZeroTAM danışmanlığını ve ZeroPEN penetrasyon testini tamamlar.

Neden değişmez depolama? Modern ransomware saldırılarının ortak paydası, üretim ortamını şifrelemeden önce backup'ları bulup yok etmektir. Yazılabilir bir repository, yeterli yetkiye sahip bir saldırgan için yalnızca bir hedeftir. ZeroVault, yetkinin kendisini önemsiz hale getirir: silme komutu çalışır, ama veri yerinde kalır.

Dört katman, sıfır taviz

ZeroVault, BackupSec ailesinin geri kalanıyla birlikte çalışır:

Hizmet	Roİ
ZeroMON	Gözlemlenebilirlik platformu — gerçek zamanlı izleme ve güvenlik sinyalleri
ZeroTAM	Uzman danışmanlık — mimari, kapasite, strateji ve kriz desteği
ZeroPEN	Penetrasyon testi & kurtarma kanıtı — backup'ları bir saldırganın yapacağı gibi test eder
ZeroVault	Bulut depolama hizmeti — silinemeyen veya şifrelenemeyen bir son kopya (bu belge)

Kimler için?

- 3-2-1-1-0 kuralındaki değişmez bulut kopyasını eksiksiz uygulamak isteyen Veeam kullanıcıları
- Donanım yönetmeden, hizmet olarak değişmez depolama isteyen kuruluşlar
- Ransomware'e karşı son savunma hattını güvence altına alan kuruluşlar
- Mevzuata dayalı saklama süreleri için değişmez bir bulut arşivine ihtiyaç duyan kuruluşlar
- Maliyeti öngörülebilir, egress ücreti olmayan bulut depolama arayan IT ekipleri
- BDDK / SPK / DORA / KVKK / GDPR yükümlülükleri olan kuruluşlar

2. Bulut Mimarisi & Teknik Özellikler

Bir bulut depolama hizmeti olarak ZeroVault'un teknik özellikleri:

Alan	Teknik Özellik
Dağıtım Modeli	Tümüyle yönetilen bulut depolama hizmeti — satın alınacak, kurulacak veya bakımı yapılacak donanım yok; dakikalar içinde devreye alınır
Değişmezlik	Object Lock (WORM), governance & compliance modu, yapılandırılabilir saklama süresi (gün/yıl), legal hold desteği
Mimari İzolasyon	Üretim açısından mantıksal air-gap, ayrı kimlik bilgileri/IAM, write-once-read-many zorunluluğu
Protokol & Entegrasyon	Amazon S3 API uyumlu; Veeam Backup & Replication ve Veeam Data Platform ile yerel entegrasyon
Veeam Repository Modu	Doğrudan nesne depolama repository'si olarak veya SOBR kapasite/performans katmanı olarak kullanılabilir
Veri Dayanıklılığı	On bir dokuz (99.999999999%) dayanıklılık, birden fazla availability zone genelinde replike edilir
Coğrafi Kapsam	Çok bölgeli bulut dağıtım seçenekleri — veri konumlandırma ihtiyaçları için bölge seçin
Şifreleme	Aktarım sırasında ve beklemede AES-256 şifreleme
Maliyet Öngörülebilirliği	Gizli egress veya API çağrısı ücreti olmayan öngörülebilir bulut depolama ekonomisi
Uyumluluk Duruşu	HIPAA, GDPR, PCI-DSS ve SOC 2 Type II gereksinimleriyle uyumlu bulut altyapısı
Yönetim	Merkezi web konsolu, BackupSec markalı erişim, API tabanlı provizyon — yönetilecek sunucu yok

3. Veeam Entegrasyonu

ZeroVault, Veeam Backup & Replication ile iki şekilde kullanılabilir:

- 1 Doğrudan Nesne Depolama Repository'si — backup işleri doğrudan ZeroVault'a yazar.
- 2 SOBR Kapasite/Performans Katmanı — Scale-Out Backup Repository yapılandırmasında eski geri yükleme noktalarının otomatik olarak aktarıldığı değişmez katman olarak kullanılır.

Mantıksal air-gap: ZeroVault erişim kimlik bilgileri, Veeam yönetim düzleminde ve Active Directory'den ayrı olarak yönetilir. AD ele geçirilse bile, ZeroVault'a doğrudan yıkıcı bir yol yoktur.

4. Kullanım Senaryoları

Senaryo	Açıklama
Son Kopya Dayanıklılığı	3-2-1-1-0 kuralının "1" (değişmez) ve "0" (doğrulanmış geri yükleme) bileşenlerini karşılayan son savunma hattı
Ransomware'e Dayanıklı Repository	Bir saldırgan domain admin yetkileri elde etse bile silinemeyen veya şifrelenemeyen bir backup kopyası
Uyumluluk Arşivi	Mevzuata dayalı saklama sürelerini karşılayan değişmez uzun vadeli arşiv
Felaket Kurtarma Bulut Katmanı	Tesis dışı / bulut DR kopyası için maliyeti öngörülebilir depolama

5. Mevzuat Kapsamı

Mevzuat	ZeroVault'un Desteklediği Gereksinimler
BDDK	Art.45 backup, BT.31 ransomware kontrolleri — değişmez bir son kopya
SPK III-35.1	Veri saklama süreleri, iş sürekliliği için değişmez arşiv
DORA (EU)	Art.11-12 backup politikası — değişmez, air-gap uygulanmış kopya gereksinimi
KVKK	Art.12 teknik önlemler — kişisel verilerin değişmez & şifreli olarak depolanması
GDPR (EU)	Art.32 güvenlik önlemleri — şifreleme ve bütünlük koruması
ISO 27001 / NIST	A.12.3 backup, A.8.3 medya işleme, NIST SP 800-209 depolama güvenliği

6. Sonraki Adım

Başlamak için: BackupSec, ZeroVault'u mevcut Veeam ortamınıza bir repository veya SOBR kapasite katmanı olarak entegre etmek üzere bölge, saklama ve erişim yapılandırmasını planlamak için sizinle birlikte çalışır.