

ZeroVault

W pełni zarządzana, zgodna z S3 usługa cloud storage dla Veeam

“Zero kompromisów.” — Atakujący nigdy nie znajdzie kopii, której nie może usunąć.

Usługa	ZeroVault — Oparta na chmurze usługa niezmiennego object storage
Główny obszar	W pełni zarządzany, niezmienny cloud storage dla Veeam Backup & Replication
Wersja	1.0
Data	Czerwiec 2026
Zakres	BDDK · SPK · DORA · KVKK · GDPR · ISO 27001 · NIST
Dostawca	BackupSec

1. Czym jest ZeroVault?

ZeroVault to w pełni zarządzana usługa cloud storage stworzona specjalnie dla środowisk Veeam Backup & Replication — zgodna z S3, niezmienna i logicznie odizolowana (air-gap). Nie trzeba kupować sprzętu, przydzielać przestrzeni w centrum danych ani utrzymywać infrastruktury storage; ZeroVault jest dostarczany jako usługa chmurowa i udostępniany w ciągu kilku minut. Nawet jeśli atakujący przejmie infrastrukturę backup, uzyska uprawnienia administratora domeny i uzyska dostęp do bazy konfiguracyjnej Veeam — kopii backup w ZeroVault nie da się ani usunąć, ani zaszyfrować przed upływem okresu retencji. ZeroVault stanowi warstwę cloud storage rodziny BackupSec, uzupełniając monitorowanie ZeroMON, doradztwo ZeroTAM oraz testy penetracyjne ZeroPEN.

Dlaczego niezmienny storage? Wspólnym mianownikiem współczesnych ataków ransomware jest odnajdywanie i niszczenie backupów przed zaszyfrowaniem środowiska produkcyjnego. Repozytorium z prawem zapisu jest jedynie celem dla atakującego z odpowiednimi uprawnieniami. ZeroVault sprawia, że same uprawnienia stają się nieistotne: polecenie usunięcia zostaje wykonane, ale dane pozostają nienaruszone.

Cztery warstwy, zero kompromisów

ZeroVault działa wspólnie z pozostałymi produktami rodziny BackupSec:

Usługa	Rola
ZeroMON	Platforma obserwowalności — monitorowanie w czasie rzeczywistym i sygnały bezpieczeństwa
ZeroTAM	Doradztwo eksperckie — architektura, pojemność, strategia i wsparcie w sytuacjach kryzysowych
ZeroPEN	Test penetracyjny & dowód odtwarzalności — testuje backupy tak, jak zrobiłby to atakujący
ZeroVault	Usługa cloud storage — ostatnia kopia, której nie można usunąć ani zaszyfrować (niniejszy dokument)

Dla kogo?

- Użytkownicy Veeam, którzy chcą w pełni wdrożyć niezmienną kopię w chmurze w ramach reguły 3-2-1-1-0
- Organizacje, które chcą korzystać z niezmiennego storage jako usługi, bez zarządzania sprzętem
- Organizacje zabezpieczające ostatnią linię obrony przed ransomware
- Organizacje potrzebujące niezmiennego archiwum w chmurze na potrzeby regulacyjnych okresów retencji
- Zespoły IT poszukujące cloud storage o przewidywalnych kosztach, bez opłat za egress
- Organizacje objęte obowiązkami BDDK / SPK / DORA / KVKK / GDPR

2. Architektura chmury & specyfikacja techniczna

Specyfikacja techniczna ZeroVault jako usługi cloud storage:

Obszar	Specyfikacja
Model wdrożenia	W pełni zarządzana usługa cloud storage — bez sprzętu do kupienia, instalacji czy utrzymania; udostępniana w ciągu kilku minut
Niezmiennność	Object Lock (WORM), tryb governance & compliance, konfigurowalny okres retencji (dni/lata), obsługa legal hold
Izolacja architektoniczna	Logiczny air-gap od sieci produkcyjnej, oddzielne poświadczenia/IAM, egzekwowanie zasady write-once-read-many
Protokół & integracja	Zgodność z Amazon S3 API; natywna integracja z Veeam Backup & Replication oraz Veeam Data Platform
Tryb repozytorium Veeam	Możliwość użycia jako bezpośrednie repozytorium object storage lub jako warstwa pojemności/wydajności SOBR
Trwałość danych	Trwałość na poziomie jedenastu dziewiątek (99.999999999%), replikacja w wielu strefach dostępności
Zasięg geograficzny	Opcje wdrożenia chmurowego w wielu regionach — wybór regionu zgodnie z potrzebami rezydencji danych
Szyfrowanie	Szyfrowanie AES-256 w transzycie i w spoczynku
Przewidywalność kosztów	Przewidywalna ekonomika cloud storage bez ukrytych opłat za egress czy wywołania API
Poziom zgodności	Infrastruktura chmurowa zgodna z wymogami HIPAA, GDPR, PCI-DSS oraz SOC 2 Type II
Zarządzanie	Scentralizowana konsola webowa, dostęp w marce BackupSec, udostępnianie sterowane przez API — brak serwerów do zarządzania

3. Integracja z Veeam

ZeroVault można wykorzystać z Veeam Backup & Replication na dwa sposoby:

- 1 Bezpośrednie repozytorium object storage — zadania backupu zapisują dane bezpośrednio do ZeroVault.
- 2 Warstwa pojemności/wydajności SOBR — wykorzystywana jako niezmienna warstwa, do której automatycznie przenoszone są starsze punkty przywracania w konfiguracji Scale-Out Backup Repository.

Logiczny air-gap: Poświadczenia dostępu do ZeroVault są zarządzane oddzielnie od warstwy zarządzania Veeam oraz Active Directory. Nawet w przypadku przejęcia AD nie istnieje bezpośrednia destrukcyjna ścieżka do ZeroVault.

4. Przypadki użycia

Scenariusz	Opis
Odporność ostatniej kopii	Ostatnia linia obrony spełniająca komponenty “1” (niezmiennność) i “0” (zweryfikowane odtwarzanie) reguły 3-2-1-1-0
Repozytorium odporne na ransomware	Kopia backup, której nie można usunąć ani zaszyfrować, nawet jeśli atakujący uzyska uprawnienia administratora domeny
Archiwum zgodności	Niezmiennie archiwum długoterminowe spełniające regulacyjne okresy retencji
Chmurowa warstwa Disaster Recovery	Storage o przewidywalnych kosztach dla kopii DR poza siedzibą / w chmurze

5. Zakres regulacyjny

Regulacja	Wymogi wspierane przez ZeroVault
BDDK	Art.45 backup, BT.31 mechanizmy kontroli ransomware — niezmienna ostatnia kopia
SPK III-35.1	Okresy retencji danych, niezmiennie archiwum na potrzeby ciągłości działania
DORA (EU)	Art.11-12 polityka backupu — wymóg niezmiennnej kopii z air-gap
KVKK	Art.12 środki techniczne — niezmiennie & szyfrowane przechowywanie danych osobowych
GDPR (EU)	Art.32 środki bezpieczeństwa — szyfrowanie i ochrona integralności
ISO 27001 / NIST	A.12.3 backup, A.8.3 postępowanie z nośnikami, NIST SP 800-209 bezpieczeństwo storage

6. Następny krok

Aby rozpocząć: BackupSec współpracuje z Tobą przy planowaniu konfiguracji regionu, retencji i dostępu w celu zintegrowania ZeroVault z Twoim istniejącym środowiskiem Veeam jako repozytorium lub warstwa pojemności SOBR.