ZeroMON

Veeam 백업 인프라를 위한 실시간 모니터링 & 보안 플랫폼

“모든 것을 보고, 아무것도 놓치지 마십시오.” — 복구 시점 이전에 장애를 포착합니다.

서비스	ZeroMON — 백업 옵저버빌리티 플랫폼
중점 영역	Veeam Backup & Replication 모니터링, 보안 신호 및 용량 분석
버전	1.0
날짜	2026년 6월
적용 범위	BDDK · SPK · DORA · KVKK · GDPR · ISO 27001 · NIST
제공자	BackupSec

1. ZeroMON이란?

ZeroMON은 백업 인프라를 위한 통합 옵저버빌리티 플랫폼입니다. 백업 작업, 보안 점검, Veeam 대응 가시성을 한곳에서 모니터링합니다. 백업 팀, MSP, 운영 팀을 위해 설계되어 복구 시점 이전에 장애, 구성 드리프트, 랜섬웨어 복구 위험을 탐지합니다. ZeroMON은 BackupSec 제품군의 모니터링 계층으로, ZeroTAM 전문가 자문, ZeroPEN 침투 테스트, ZeroVault 클라우드 스토리지를 보완합니다.

> **왜 ZeroMON인가?** 모든 백업 시스템은 복구 시점이 되기 전까지는 정상으로 보입니다. ZeroMON은 실패한 작업, 구성 드리프트, 취약한 불변성 제어, 그리고 잘못된 확신을 — 사고가 되기 전에 포착합니다.

4개 계층, 타협 없음

ZeroMON은 나머지 BackupSec 제품군과 함께 작동합니다:

서비스	역할
ZeroMON	**옵저버빌리티 플랫폼 — 실시간 모니터링 및 보안 신호 (본 문서)**
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

누구를 위한 제품인가?

- 복구 시점 이전에 장애, 드리프트, 랜섬웨어 위험을 탐지해야 하는 백업 팀
- 멀티테넌트 환경을 관리하는 MSP 및 서비스 제공업체
- Veeam 기반 인프라를 운영하는 운영 팀
- 스프레드시트 대신 원클릭 컴플라이언스 보고서를 원하는 감사 & 보안 팀
- BDDK / SPK / DORA / KVKK / GDPR 의무가 있는 조직

2. 모니터링 적용 범위 카탈로그

ZeroMON은 백업 환경의 다음 영역을 실시간으로 지속 모니터링합니다:

모니터링 영역	내용
작업 모니터링 & SLA 추적	백업/복제 작업의 성공/실패 상태, 재시도, 지연 및 SLA 위반 탐지
리포지토리 & 용량 모니터링	사용률, 증가 추세, “포화 예상 시점(time-to-full)” 예측, 스토리지 성능
구성 드리프트 & 변경 탐지	작업, 리포지토리 및 권한 구성 변경에 대한 주체/내용/시점 추적
보안 이벤트 탐지	의심스러운 삭제/암호화 행위, 무단 접근 시도, 이상 징후 기반 경보
불변성 & 하드닝 상태	Object Lock / 하드닝된 리포지토리 상태의 지속적 검증, 불변성 기간 추적
Veeam 구성 요소 상태	VBR 서버, 프록시, 리포지토리 및 Veeam 서비스의 실시간 상태
멀티테넌트 뷰	MSP를 위한 고객별 대시보드, 역할 기반 접근 및 격리된 보고
컴플라이언스 & 경영진 보고	원클릭 BDDK/SPK/DORA/KVKK/GDPR/ISO 컴플라이언스 및 복구 준비 상태 보고서
경보 & 알림 연동	이메일, 웹훅 및 SIEM 연동을 통한 즉각적인 경보 라우팅
읽기 전용 접근 & 데이터 레지던시	온프레미스 배포, 읽기 전용 API 접근, 데이터가 네트워크를 벗어나지 않음(제로 데이터 유출)

3. 배포 & 라이프사이클

ZeroMON은 클라이언트로서 온프레미스에 배포되며 프로덕션 환경에 대한 변경을 요구하지 않습니다. 일반적인 라이프사이클:

단계	내용
배포	고객 패널에서 OVA 클라이언트를 다운로드하여 자체 환경에 배포 — 프로덕션 변경 불필요
연결	읽기 전용 사용자 계정으로 백업 애플리케이션에 연결
기준선 설정 & 보정	임계값 설정 및 초기 시스템 상태 점수(System Health Score) 산정
실시간 모니터링 (24/7)	실시간 대시보드, 즉각적인 경보 및 포렌식 로깅
정기 보고	경영진 및 감사자를 위한 컴플라이언스 & 복구 준비 상태 보고서

> **데이터 레지던시 약속:** ZeroMON은 온프레미스에서 실행되며, 백업 데이터, 텔레메트리, 구성 정보가 네트워크를 벗어나지 않습니다. 연결은 읽기 전용 API 접근을 통해 이루어집니다 — 제로 데이터 유출.

4. 주요 기능

실시간 운영 대시보드

전체 백업 인프라에 걸친 실시간 작업 추적, 캘린더 뷰 및 자동화된 백업 보안 점검.

포렌식 인텔리전스

구성 변경, 의심스러운 행위 및 중요한 보안 이벤트에 대한 즉각적인 경보를 갖춘 완전한 감사 추적.

용량 분석

용량 위기가 발생하기 전에 이를 예방하는 증가 예측 및 “포화 예상 시점” 전망.

경영진 보고서

경영진 및 감사자를 위한 원클릭 컴플라이언스 및 복구 준비 상태 보고서 — 스프레드시트 불필요.

5. 산출물

1. 실시간 운영 대시보드 — 작업, 용량 및 보안 상태의 실시간 조회.
2. 포렌식 감사 로그 — 구성 변경 및 의심스러운 행위에 대한 완전한 감사 추적.
3. 용량 분석 보고서 — 증가 예측 및 “포화 예상 시점” 전망.
4. 컴플라이언스 & 경영진 보고서 — 원클릭, 감사 대응 형식.
5. 즉각적인 경보 — 이메일 / 웹훅 / SIEM 연동을 통해.
6. 멀티테넌트 대시보드 — MSP를 위한 격리된 고객별 조회.

6. 규제 적용 범위

규제	ZeroMON이 지원하는 요구사항
BDDK	Art.45 백업, Art.51 지속 모니터링 요건, BT.31 랜섬웨어 탐지
SPK III-35.1	비즈니스 연속성 모니터링 및 보고
DORA (EU)	Art.11-12 백업 정책 모니터링, Art.17 지속 테스트 증적
KVKK	Art.12 기술적 조치 — 접근 & 변경 로깅
GDPR (EU)	Art.32 보안 조치 — 지속 모니터링 증적
ISO 27001 / NIST	A.12.3 백업, A.12.4 로깅 & 모니터링, CSF DE (Detect)

7. 다음 단계

시작하려면: BackupSec는 기존 Veeam 환경에서 ZeroMON을 몇 분 내에 가동할 수 있도록 배포(OVA) 및 읽기 전용 연결 단계를 함께 계획합니다.