

ZeroMON

Real-Time Monitoring & Security Platform for Veeam Backup Infrastructure

“See everything. Miss nothing.” — Failures get caught before restore time.

Service	ZeroMON — Backup Observability Platform
Focus	Veeam Backup & Replication monitoring, security signals and capacity analytics
Version	1.0
Date	June 2026
Coverage	BDDK · SPK · DORA · KVKK · GDPR · ISO 27001 · NIST
Provider	BackupSec

1. What is ZeroMON?

ZeroMON is a unified observability platform for your backup infrastructure: it monitors backup jobs, security checks, and Veeam-ready visibility from one place. Built for backup teams, MSPs, and operations teams, it detects failures, configuration drift, and ransomware recovery risk BEFORE restore time. ZeroMON is the monitoring layer of the BackupSec family, complementing ZeroTAM expert advisory, ZeroPEN penetration testing, and ZeroVault cloud storage.

Why ZeroMON? Every backup system looks fine until recovery time. ZeroMON catches failed jobs, configuration drift, weak immutability controls, and false confidence — before they become incidents.

Four layers, zero compromise

ZeroMON works alongside the rest of the BackupSec family:

Service	Role
ZeroMON	Observability platform — real-time monitoring and security signals (this document)
ZeroTAM	Expert advisory — architecture, capacity, strategy and crisis support
ZeroPEN	Penetration test & recovery proof — tests backups the way an attacker would
ZeroVault	Cloud storage service — a last copy that cannot be deleted or encrypted

Who is it for?

- Backup teams who need to detect failures, drift, and ransomware risk before restore time
- MSPs and service providers managing multi-tenant environments
- Operations teams running Veeam-based infrastructure
- Audit & security teams who want one-click compliance reports instead of spreadsheets
- Organizations with BDDK / SPK / DORA / KVKK / GDPR obligations

2. Monitoring Coverage Catalog

ZeroMON continuously monitors the following areas of your backup environment in real time:

Monitoring Area	Content
Job Monitoring & SLA Tracking	Backup/replication job success/failure status, retries, delays, and SLA-breach detection
Repository & Capacity Monitoring	Fill rate, growth trend, "time-to-full" forecast, storage performance
Configuration Drift & Change Detection	Tracking who/what/when for changes to job, repository and permission configuration
Security Event Detection	Suspicious deletion/encryption behavior, unauthorized access attempts, anomaly-based alerts
Immutability & Hardening Status	Continuous verification of Object Lock / hardened-repo status, immutability-period tracking
Veeam Component Health	Live health status of the VBR server, proxies, repositories and Veeam services
Multi-Tenant View	Per-client dashboard, role-based access and isolated reporting for MSPs
Compliance & Executive Reporting	One-click BDDK/SPK/DORA/KVKK/GDPR/ISO compliance and recovery-readiness reports
Alerting & Notification Integration	Instant alert routing via email, webhook and SIEM integration
Read-Only Access & Data Residency	On-premise deployment, read-only API access, data never leaves your network (zero data exfiltration)

3. Deployment & Lifecycle

ZeroMON is deployed on-premise as a client; it requires no changes to your production environment. The typical lifecycle:

Stage	Content
Deployment	Downloading the OVA client from the customer panel and deploying it in your own environment — no production changes required
Connection	Connecting to your backup applications with a read-only user account
Baseline & Calibration	Setting thresholds and establishing the initial System Health Score
Live Monitoring (24/7)	Real-time dashboard, instant alerts and forensic logging
Periodic Reporting	Compliance & recovery-readiness reports ready for management and auditors

Data residency commitment: ZeroMON runs on-premise; backup data, telemetry, and configuration information never leave your network. Connections are established via read-only API access — zero data exfiltration.

4. Key Features

Live Operations Dashboard

Real-time job tracking, calendar views, and automated backup security checks across your entire backup infrastructure.

Forensic Intelligence

Complete audit trails with instant alerts for configuration changes, suspicious behavior, and critical security events.

Capacity Analytics

Growth forecasts and “time-to-full” projections that prevent capacity crises before they happen.

Executive Reports

One-click compliance and recovery readiness reports ready for management and auditors — no spreadsheets required.

5. Deliverables

- 1 Live Operations Dashboard — real-time view of job, capacity, and security status.
- 2 Forensic Audit Log — complete audit trail for configuration changes and suspicious behavior.
- 3 Capacity Analytics Report — growth forecast and “time-to-full” projection.
- 4 Compliance & Executive Reports — one click, audit-ready format.
- 5 Instant Alerts — via email / webhook / SIEM integration.
- 6 Multi-Tenant Dashboard — isolated, per-client view for MSPs.

6. Regulatory Coverage

Regulation	Requirements ZeroMON Supports
BDDK	Art.45 backup, Art.51 continuous monitoring expectation, BT.31 ransomware detection
SPK III-35.1	Business continuity monitoring and reporting
DORA (EU)	Art.11-12 backup policy monitoring, Art.17 continuous test evidence
KVKK	Art.12 technical measures — access & change logging
GDPR (EU)	Art.32 security measures — continuous monitoring evidence
ISO 27001 / NIST	A.12.3 backup, A.12.4 logging & monitoring, CSF DE (Detect)

7. Next Step

To get started: BackupSec works with you to plan the deployment (OVA) and read-only connection steps to bring ZeroMON online in your existing Veeam environment within minutes.