ZeroMON

面向 Veeam 备份基础设施的实时监控 & 安全平台

“看见一切，绝不遗漏。” — 故障在恢复时刻到来之前即被捕获。

服务	ZeroMON — 备份可观测性平台
聚焦	Veeam Backup & Replication 监控、安全信号与容量分析
版本	1.0
日期	2026年6月
覆盖范围	BDDK · SPK · DORA · KVKK · GDPR · ISO 27001 · NIST
提供方	BackupSec

1. 什么是 ZeroMON?

ZeroMON 是面向您备份基础设施的统一可观测性平台：它在一处即可监控备份作业、安全检查以及面向 Veeam 的可视化。它专为备份团队、MSP 和运维团队打造，能够在恢复时刻到来之前检测故障、配置漂移以及勒索软件恢复风险。ZeroMON 是 BackupSec 家族的监控层，与 ZeroTAM 专家咨询、ZeroPEN 渗透测试和 ZeroVault 云存储互为补充。

> **为什么选择 ZeroMON?** 每一套备份系统在真正恢复之前看起来都完好无缺。ZeroMON 能在故障作业、配置漂移、薄弱的不可变控制以及虚假的安全感演变为事故之前 — 将它们一一捕获。

四层防护，零妥协

ZeroMON 与 BackupSec 家族的其余成员协同工作：

服务	角色
ZeroMON	**可观测性平台 — 实时监控与安全信号（本文档）**
ZeroTAM	专家咨询 — 架构、容量、策略与危机支持
ZeroPEN	渗透测试 & 恢复验证 — 以攻击者的方式测试备份
ZeroVault	云存储服务 — 一份无法被删除或加密的最后副本

适用于谁?

- 需要在恢复时刻到来之前检测故障、漂移和勒索软件风险的备份团队
- 管理多租户环境的 MSP 和服务提供商
- 运行基于 Veeam 基础设施的运维团队
- 希望一键生成合规报告而非依赖电子表格的审计 & 安全团队
- 负有 BDDK / SPK / DORA / KVKK / GDPR 合规义务的组织

2. 监控覆盖目录

ZeroMON 实时持续监控您备份环境的以下领域：

监控领域	内容
作业监控 & SLA 跟踪	备份/复制作业的成功/失败状态、重试、延迟以及 SLA 违约检测
存储库 & 容量监控	填充率、增长趋势、“写满时间”预测、存储性能
配置漂移 & 变更检测	跟踪作业、存储库和权限配置的变更（谁/做了什么/何时）
安全事件检测	可疑的删除/加密行为、未经授权的访问尝试、基于异常的告警
不可变 & 加固状态	持续验证 Object Lock / 加固存储库状态，跟踪不可变周期
Veeam 组件健康状况	VBR 服务器、代理、存储库和 Veeam 服务的实时健康状态
多租户视图	面向 MSP 的按客户划分仪表板、基于角色的访问以及隔离式报告
合规 & 高管报告	一键生成 BDDK/SPK/DORA/KVKK/GDPR/ISO 合规与恢复就绪报告
告警 & 通知集成	通过电子邮件、webhook 和 SIEM 集成即时路由告警
只读访问 & 数据驻留	本地部署、只读 API 访问，数据绝不离开您的网络（零数据外泄）

3. 部署 & 生命周期

ZeroMON 作为客户端在本地部署；它无需更改您的生产环境。典型的生命周期如下：

阶段	内容
部署	从客户面板下载 OVA 客户端并将其部署到您自己的环境中 — 无需更改生产环境
连接	使用只读用户账户连接到您的备份应用
基线 & 校准	设置阈值并建立初始的系统健康评分
实时监控（24/7）	实时仪表板、即时告警和取证日志记录
定期报告	为管理层和审计人员准备的合规 & 恢复就绪报告

> **数据驻留承诺：** ZeroMON 在本地运行；备份数据、遥测数据和配置信息绝不离开您的网络。连接通过只读 API 访问建立 — 零数据外泄。

4. 核心功能

实时运维仪表板
在您的整个备份基础设施中提供实时作业跟踪、日历视图和自动化备份安全检查。

取证情报
完整的审计跟踪，并针对配置变更、可疑行为和关键安全事件提供即时告警。

容量分析
增长预测和“写满时间”推算，在容量危机发生之前予以防范。

高管报告
一键生成面向管理层和审计人员的合规与恢复就绪报告 — 无需电子表格。

5. 交付物

1. 实时运维仪表板 — 实时查看作业、容量和安全状态。
2. 取证审计日志 — 针对配置变更和可疑行为的完整审计跟踪。
3. 容量分析报告 — 增长预测和“写满时间”推算。
4. 合规 & 高管报告 — 一键生成，符合审计要求的格式。
5. 即时告警 — 通过电子邮件 / webhook / SIEM 集成。
6. 多租户仪表板 — 面向 MSP 的隔离式、按客户划分的视图。

6. 法规覆盖

法规	ZeroMON 支持的要求
BDDK	Art.45 备份、Art.51 持续监控要求、BT.31 勒索软件检测
SPK III-35.1	业务连续性监控与报告
DORA (EU)	Art.11-12 备份策略监控、Art.17 持续测试证据
KVKK	Art.12 技术措施 — 访问 & 变更日志记录
GDPR (EU)	Art.32 安全措施 — 持续监控证据
ISO 27001 / NIST	A.12.3 备份、A.12.4 日志记录 & 监控、CSF DE (Detect)

7. 下一步

> **如何开始：** BackupSec 将与您共同规划部署 (OVA) 和只读连接步骤，在几分钟内让 ZeroMON 在您现有的 Veeam 环境中上线。