ZeroMON

Echtzeit-Monitoring- & Security-Plattform für Veeam-Backup-Infrastruktur

“Alles im Blick. Nichts übersehen.” — Fehler werden erkannt, bevor die Wiederherstellung ansteht.

Service	ZeroMON — Backup-Observability-Plattform
Fokus	Monitoring von Veeam Backup & Replication, Sicherheitssignale und Kapazitätsanalysen
Version	1.0
Datum	Juni 2026
Abdeckung	BDDK · SPK · DORA · KVKK · GDPR · ISO 27001 · NIST
Anbieter	BackupSec

1. Was ist ZeroMON?

ZeroMON ist eine einheitliche Observability-Plattform für Ihre Backup-Infrastruktur: Sie überwacht Backup-Jobs, Sicherheitsprüfungen und Veeam-fähige Transparenz an einem zentralen Ort. Entwickelt für Backup-Teams, MSPs und Operations-Teams, erkennt sie Fehler, Konfigurationsabweichungen und das Risiko einer Ransomware-Wiederherstellung, BEVOR die Wiederherstellung ansteht. ZeroMON ist die Monitoring-Ebene der BackupSec-Familie und ergänzt die Expertenberatung ZeroTAM, das Penetrationstesting ZeroPEN und den Cloud-Storage ZeroVault.

> **Warum ZeroMON?** Jedes Backup-System sieht bis zur Wiederherstellung gut aus. ZeroMON erkennt fehlgeschlagene Jobs, Konfigurationsabweichungen, schwache Immutability-Kontrollen und trügerische Sicherheit — bevor daraus Vorfälle werden.

Vier Ebenen, null Kompromisse

ZeroMON arbeitet Hand in Hand mit dem Rest der BackupSec-Familie:

Service	Rolle
ZeroMON	**Observability-Plattform — Echtzeit-Monitoring und Sicherheitssignale (dieses Dokument)**
ZeroTAM	Expertenberatung — Architektur, Kapazität, Strategie und Krisenunterstützung
ZeroPEN	Penetrationstest & Wiederherstellungsnachweis — testet Backups so, wie es ein Angreifer tun würde
ZeroVault	Cloud-Storage-Dienst — eine letzte Kopie, die nicht gelöscht oder verschlüsselt werden kann

Für wen ist es gedacht?

- Backup-Teams, die Fehler, Abweichungen und Ransomware-Risiken vor der Wiederherstellung erkennen müssen
- MSPs und Service-Provider, die mandantenfähige Umgebungen verwalten
- Operations-Teams, die eine Veeam-basierte Infrastruktur betreiben
- Audit- & Security-Teams, die Ein-Klick-Compliance-Berichte statt Tabellenkalkulationen wollen
- Organisationen mit BDDK- / SPK- / DORA- / KVKK- / GDPR-Verpflichtungen

2. Katalog der Überwachungsabdeckung

ZeroMON überwacht die folgenden Bereiche Ihrer Backup-Umgebung kontinuierlich in Echtzeit:

Überwachungsbereich	Inhalt
Job-Monitoring & SLA-Tracking	Erfolgs-/Fehlerstatus von Backup-/Replikations-Jobs, Wiederholungen, Verzögerungen und Erkennung von SLA-Verletzungen
Repository- & Kapazitäts-Monitoring	Füllstand, Wachstumstrend, “time-to-full”-Prognose, Storage-Performance
Konfigurationsabweichung & Änderungserkennung	Nachverfolgung von Wer/Was/Wann bei Änderungen an Job-, Repository- und Berechtigungskonfigurationen
Erkennung von Sicherheitsereignissen	Verdächtiges Lösch-/Verschlüsselungsverhalten, unbefugte Zugriffsversuche, anomaliebasierte Warnmeldungen
Immutability- & Hardening-Status	Kontinuierliche Überprüfung des Object-Lock- / Hardened-Repo-Status, Nachverfolgung des Immutability-Zeitraums
Zustand der Veeam-Komponenten	Live-Zustandsstatus des VBR-Servers, der Proxies, Repositories und Veeam-Dienste
Mandantenfähige Ansicht	Dashboard pro Kunde, rollenbasierter Zugriff und isoliertes Reporting für MSPs
Compliance- & Management-Reporting	Ein-Klick-Berichte zu BDDK/SPK/DORA/KVKK/GDPR/ISO-Compliance und Wiederherstellungsbereitschaft
Alerting- & Benachrichtigungsintegration	Sofortige Weiterleitung von Warnmeldungen per E-Mail, Webhook und SIEM-Integration
Read-Only-Zugriff & Datenresidenz	On-Premise-Bereitstellung, Read-Only-API-Zugriff, Daten verlassen niemals Ihr Netzwerk (keine Datenexfiltration)

3. Bereitstellung & Lebenszyklus

ZeroMON wird on-premise als Client bereitgestellt; es sind keine Änderungen an Ihrer Produktionsumgebung erforderlich. Der typische Lebenszyklus:

Phase	Inhalt
Bereitstellung	Herunterladen des OVA-Clients aus dem Kundenportal und Bereitstellung in Ihrer eigenen Umgebung — keine Änderungen an der Produktion erforderlich
Verbindung	Verbindung zu Ihren Backup-Anwendungen mit einem Read-Only-Benutzerkonto
Baseline & Kalibrierung	Festlegen von Schwellenwerten und Ermittlung des initialen System Health Score
Live-Monitoring (24/7)	Echtzeit-Dashboard, sofortige Warnmeldungen und forensisches Logging
Regelmäßiges Reporting	Compliance- & Wiederherstellungsberichte, fertig für Management und Auditoren

> **Zusage zur Datenresidenz:** ZeroMON läuft on-premise; Backup-Daten, Telemetrie und Konfigurationsinformationen verlassen niemals Ihr Netzwerk. Verbindungen werden über Read-Only-API-Zugriff hergestellt — keine Datenexfiltration.

4. Wichtige Funktionen

Live-Betriebs-Dashboard

Echtzeit-Job-Tracking, Kalenderansichten und automatisierte Backup-Sicherheitsprüfungen über Ihre gesamte Backup-Infrastruktur hinweg.

Forensische Intelligenz

Vollständige Audit-Trails mit sofortigen Warnmeldungen bei Konfigurationsänderungen, verdächtigem Verhalten und kritischen Sicherheitsereignissen.

Kapazitätsanalysen

Wachstumsprognosen und “time-to-full”-Projektionen, die Kapazitätsengpässe verhindern, bevor sie entstehen.

Management-Berichte

Ein-Klick-Berichte zu Compliance und Wiederherstellungsbereitschaft, fertig für Management und Auditoren — keine Tabellenkalkulationen erforderlich.

5. Liefergegenstände

1. Live-Betriebs-Dashboard — Echtzeitansicht von Job-, Kapazitäts- und Sicherheitsstatus.
2. Forensisches Audit-Log — vollständiger Audit-Trail für Konfigurationsänderungen und verdächtiges Verhalten.
3. Kapazitätsanalyse-Bericht — Wachstumsprognose und “time-to-full”-Projektion.
4. Compliance- & Management-Berichte — ein Klick, audit-fertiges Format.
5. Sofortige Warnmeldungen — per E-Mail / Webhook / SIEM-Integration.
6. Mandantenfähiges Dashboard — isolierte Ansicht pro Kunde für MSPs.

6. Regulatorische Abdeckung

Regulierung	Von ZeroMON unterstützte Anforderungen
BDDK	Art.45 Backup, Art.51 Erwartung an kontinuierliches Monitoring, BT.31 Ransomware-Erkennung
SPK III-35.1	Monitoring und Reporting zur Geschäftskontinuität
DORA (EU)	Art.11-12 Überwachung der Backup-Richtlinie, Art.17 kontinuierlicher Testnachweis
KVKK	Art.12 technische Maßnahmen — Zugriffs- & Änderungsprotokollierung
GDPR (EU)	Art.32 Sicherheitsmaßnahmen — Nachweis kontinuierlichen Monitorings
ISO 27001 / NIST	A.12.3 Backup, A.12.4 Logging & Monitoring, CSF DE (Detect)

7. Nächster Schritt

So starten Sie: BackupSec plant gemeinsam mit Ihnen die Bereitstellung (OVA) und die Read-Only-Verbindungsschritte, um ZeroMON innerhalb weniger Minuten in Ihrer bestehenden Veeam-Umgebung in Betrieb zu nehmen.