ZeroMON

Veeam バックアップインフラ向けリアルタイムモニタリング & セキュリティプラットフォーム

“すべてを可視化。見逃しゼロ。” — 障害はリストア時ではなく事前に検知されます。

サービス	ZeroMON — バックアップオブザーバビリティプラットフォーム
重点領域	Veeam Backup & Replication のモニタリング、セキュリティシグナル、キャパシティ分析
バージョン	1.0
日付	2026年6月
対応範囲	BDDK · SPK · DORA · KVKK · GDPR · ISO 27001 · NIST
プロバイダー	BackupSec

1. ZeroMON とは？

ZeroMON は、バックアップインフラのための統合オブザーバビリティプラットフォームです。バックアップジョブ、セキュリティチェック、そして Veeam に対応した可視性を一元的にモニタリングします。バックアップチーム、MSP、運用チームのために設計されており、障害、構成ドリフト、ランサムウェアからのリカバリリスクを、リストア時ではなく事前に検知します。ZeroMON は BackupSec ファミリーのモニタリングレイヤーであり、ZeroTAM のエキスパートアドバイザリー、ZeroPEN のペネトレーションテスト、ZeroVault のクラウドストレージを補完します。

> **なぜ ZeroMON なのか？** どのバックアップシステムも、リカバリの瞬間までは問題なく見えます。ZeroMON は、失敗したジョブ、構成ドリフト、脆弱なイミュータビリティ制御、そして誤った安心感を — インシデントになる前に捉えます。

4つのレイヤー、妥協ゼロ

ZeroMON は BackupSec ファミリーの他の製品と連携して機能します：

サービス	役割
ZeroMON	**オブザーバビリティプラットフォーム — リアルタイムモニタリングとセキュリティシグナル（本書）**
ZeroTAM	エキスパートアドバイザリー — アーキテクチャ、キャパシティ、戦略、危機対応サポート
ZeroPEN	ペネトレーションテスト & リカバリ実証 — 攻撃者の視点でバックアップを検証
ZeroVault	クラウドストレージサービス — 削除も暗号化もできない最後のコピー

対象となるのは？

- リストア時ではなく事前に、障害、ドリフト、ランサムウェアリスクを検知する必要があるバックアップチーム
- マルチテナント環境を管理する MSP およびサービスプロバイダー
- Veeam ベースのインフラを運用する運用チーム
- スプレッドシートの代わりにワンクリックのコンプライアンスレポートを求める監査 & セキュリティチーム
- BDDK / SPK / DORA / KVKK / GDPR の義務を負う組織

2. モニタリング対応範囲カタログ

ZeroMON は、バックアップ環境の以下の領域をリアルタイムで継続的にモニタリングします：

モニタリング領域	内容
ジョブモニタリング & SLA トラッキング	バックアップ/レプリケーションジョブの成功/失敗ステータス、再試行、遅延、SLA 違反の検知
リポジトリ & キャパシティモニタリング	使用率、増加傾向、“time-to-full”（満杯までの時間）予測、ストレージパフォーマンス
構成ドリフト & 変更検知	ジョブ、リポジトリ、権限構成の変更について「誰が・何を・いつ」を追跡
セキュリティイベント検知	不審な削除/暗号化の挙動、不正アクセスの試み、異常検知ベースのアラート
イミュータビリティ & ハードニングステータス	Object Lock / ハードンドリポジトリのステータスの継続的な検証、イミュータビリティ期間のトラッキング
Veeam コンポーネントの稼働状態	VBR サーバー、プロキシ、リポジトリ、Veeam サービスのリアルタイムな稼働状態
マルチテナントビュー	MSP 向けの顧客別ダッシュボード、ロールベースアクセス、分離されたレポーティング
コンプライアンス & エグゼクティブレポーティング	ワンクリックの BDDK/SPK/DORA/KVKK/GDPR/ISO コンプライアンスおよびリカバリ準備状況レポート
アラート & 通知の連携	メール、Webhook、SIEM 連携による即時アラート配信
読み取り専用アクセス & データレジデンシー	オンプレミス展開、読み取り専用 API アクセス、データがネットワーク外に出ることは一切なし（データ持ち出しゼロ）

3. デプロイ & ライフサイクル

ZeroMON はクライアントとしてオンプレミスに展開され、本番環境への変更を必要としません。一般的なライフサイクルは以下のとおりです：

ステージ	内容
デプロイ	カスタマーパネルから OVA クライアントをダウンロードし、ご自身の環境に展開 — 本番環境への変更は不要
接続	読み取り専用のユーザーアカウントでバックアップアプリケーションに接続
ベースライン & キャリブレーション	しきい値を設定し、初期の System Health Score を確立
ライブモニタリング（24/7）	リアルタイムダッシュボード、即時アラート、フォレンジックロギング
定期レポーティング	経営陣および監査人向けに用意されたコンプライアンス & リカバリ準備状況レポート

> **データレジデンシーへのコミットメント：** ZeroMON はオンプレミスで動作し、バックアップデータ、テレメトリ、構成情報がネットワーク外に出ることは一切ありません。接続は読み取り専用 API アクセスを介して確立されます — データ持ち出しゼロ。

4. 主な機能

ライブオペレーションダッシュボード
バックアップインフラ全体にわたる、リアルタイムのジョブトラッキング、カレンダービュー、自動化されたバックアップセキュリティチェック。

フォレンジックインテリジェンス
構成変更、不審な挙動、重大なセキュリティイベントに対する即時アラートを備えた、完全な監査証跡。

キャパシティ分析
キャパシティ危機が発生する前に防止する、増加予測と “time-to-full”（満杯までの時間）予測。

エグゼクティブレポート
経営陣および監査人向けに用意された、ワンクリックのコンプライアンスおよびリカバリ準備状況レポート — スプレッドシートは不要。

5. 提供物

1. ライブオペレーションダッシュボード — ジョブ、キャパシティ、セキュリティステータスのリアルタイムビュー。
2. フォレンジック監査ログ — 構成変更および不審な挙動に対する完全な監査証跡。
3. キャパシティ分析レポート — 増加予測と “time-to-full”（満杯までの時間）予測。
4. コンプライアンス & エグゼクティブレポート — ワンクリック、監査対応フォーマット。
5. 即時アラート — メール / Webhook / SIEM 連携経由。
6. マルチテナントダッシュボード — MSP 向けの分離された顧客別ビュー。

6. 規制対応範囲

規制	ZeroMON が対応する要件
BDDK	Art.45 バックアップ、Art.51 継続的モニタリングの要求、BT.31 ランサムウェア検知
SPK III-35.1	事業継続性のモニタリングとレポーティング
DORA (EU)	Art.11-12 バックアップポリシーのモニタリング、Art.17 継続的テストのエビデンス
KVKK	Art.12 技術的対策 — アクセス & 変更のロギング
GDPR (EU)	Art.32 セキュリティ対策 — 継続的モニタリングのエビデンス
ISO 27001 / NIST	A.12.3 バックアップ、A.12.4 ロギング & モニタリング、CSF DE (Detect)

7. 次のステップ

始めるには： BackupSec は、既存の Veeam 環境で ZeroMON を数分でオンラインにするため、展開（OVA）および読み取り専用接続の手順を、お客様と共に計画します。