ZeroMON

Platforma monitorowania w czasie rzeczywistym & bezpieczeństwa dla infrastruktury backup Veeam

“Widź wszystko. Nie pomiń niczego.” — Awarie są wykrywane, zanim nadejdzie czas odtwarzania.

Usługa	ZeroMON — Platforma obserwowalności backupu
Główny obszar	Monitorowanie Veeam Backup & Replication, sygnały bezpieczeństwa i analiza pojemności
Wersja	1.0
Data	Czerwiec 2026
Zakres	BDDK · SPK · DORA · KVKK · GDPR · ISO 27001 · NIST
Dostawca	BackupSec

1. Czym jest ZeroMON?

ZeroMON to zunifikowana platforma obserwowalności dla Twojej infrastruktury backup: monitoruje zadania backupu, kontrole bezpieczeństwa oraz zapewnia gotową dla Veeam widoczność z jednego miejsca. Stworzony z myślą o zespołach backup, dostawcach MSP i zespołach operacyjnych, wykrywa awarie, dryf konfiguracji oraz ryzyko odtwarzania po ataku ransomware, ZANIM nadejdzie czas odtwarzania. ZeroMON stanowi warstwę monitorowania rodziny BackupSec, uzupełniając doradztwo eksperckie ZeroTAM, testy penetracyjne ZeroPEN oraz cloud storage ZeroVault.

> **Dlaczego ZeroMON?** Każdy system backupu wygląda dobrze do momentu odtwarzania. ZeroMON wychwytuje nieudane zadania, dryf konfiguracji, słabe mechanizmy niezmienności oraz złudne poczucie bezpieczeństwa — zanim przerodzą się w incydenty.

Cztery warstwy, zero kompromisów

ZeroMON działa wspólnie z pozostałymi produktami rodziny BackupSec:

Usługa	Rola
ZeroMON	**Platforma obserwowalności — monitorowanie w czasie rzeczywistym i sygnały bezpieczeństwa (niniejszy dokument)**
ZeroTAM	Doradztwo eksperckie — architektura, pojemność, strategia i wsparcie w sytuacjach kryzysowych
ZeroPEN	Test penetracyjny & dowód odtwarzalności — testuje backupy tak, jak zrobiłby to atakujący
ZeroVault	Usługa cloud storage — ostatnia kopia, której nie można usunąć ani zaszyfrować

Dla kogo?

- Zespoły backup, które muszą wykrywać awarie, dryf i ryzyko ransomware przed czasem odtwarzania
- Dostawcy MSP i usługodawcy zarządzający środowiskami wielodostępnymi (multi-tenant)
- Zespoły operacyjne utrzymujące infrastrukturę opartą na Veeam
- Zespoły audytu & bezpieczeństwa, które chcą raportów zgodności generowanych jednym kliknięciem zamiast arkuszy kalkulacyjnych
- Organizacje objęte obowiązkami BDDK / SPK / DORA / KVKK / GDPR

2. Katalog zakresu monitorowania

ZeroMON w sposób ciągły monitoruje w czasie rzeczywistym następujące obszary Twojego środowiska backup:

Obszar monitorowania	Zawartość
Monitorowanie zadań & śledzenie SLA	Status powodzenia/niepowodzenia zadań backupu/replikacji, ponowne próby, opóźnienia oraz wykrywanie naruszeń SLA
Monitorowanie repozytoriów & pojemności	Stopień zapełnienia, trend wzrostu, prognoza “czasu do zapełnienia”, wydajność storage
Dryf konfiguracji & wykrywanie zmian	Śledzenie kto/co/kiedy w odniesieniu do zmian w konfiguracji zadań, repozytoriów i uprawnień
Wykrywanie zdarzeń bezpieczeństwa	Podejrzane zachowania usuwania/szyfrowania, próby nieautoryzowanego dostępu, alerty oparte na anomaliach
Status niezmienności & hardeningu	Ciągła weryfikacja statusu Object Lock / hardened repository, śledzenie okresu niezmienności
Kondycja komponentów Veeam	Bieżący status kondycji serwera VBR, proxy, repozytoriów oraz usług Veeam
Widok wielodostępny (multi-tenant)	Pulpit dla każdego klienta, dostęp oparty na rolach i odseparowane raportowanie dla dostawców MSP
Raportowanie zgodności & dla kadry zarządzającej	Raporty zgodności BDDK/SPK/DORA/KVKK/GDPR/ISO oraz gotowości do odtwarzania generowane jednym kliknięciem
Integracja alertów & powiadomień	Natychmiastowe kierowanie alertów przez e-mail, webhook oraz integrację z SIEM
Dostęp tylko do odczytu & rezydencja danych	Wdrożenie on-premise, dostęp do API tylko do odczytu, dane nigdy nie opuszczają Twojej sieci (zero eksfiltracji danych)

3. Wdrożenie & cykl życia

ZeroMON jest wdrażany on-premise jako klient; nie wymaga żadnych zmian w środowisku produkcyjnym. Typowy cykl życia:

Etap	Zawartość
Wdrożenie	Pobranie klienta OVA z panelu klienta i wdrożenie go we własnym środowisku — bez konieczności wprowadzania zmian w środowisku produkcyjnym
Połączenie	Połączenie z aplikacjami backup przy użyciu konta użytkownika tylko do odczytu
Wartości bazowe & kalibracja	Ustawienie progów oraz ustalenie początkowego wskaźnika kondycji systemu (System Health Score)
Monitorowanie na żywo (24/7)	Pulpit w czasie rzeczywistym, natychmiastowe alerty i rejestrowanie na potrzeby analizy śledczej
Raportowanie okresowe	Raporty zgodności & gotowości do odtwarzania, gotowe dla kadry zarządzającej i audytorów

Zobowiązanie dotyczące rezydencji danych: ZeroMON działa on-premise; dane backup, telemetria oraz informacje o konfiguracji nigdy nie opuszczają Twojej sieci. Połączenia nawiązywane są przez dostęp do API tylko do odczytu — zero eksfiltracji danych.

4. Kluczowe funkcje

Pulpit operacyjny na żywo

Śledzenie zadań w czasie rzeczywistym, widoki kalendarza oraz zautomatyzowane kontrole bezpieczeństwa backupu w całej infrastrukturze backup.

Analityka śledcza

Kompletne ścieżki audytu z natychmiastowymi alertami o zmianach konfiguracji, podejrzanych zachowaniach i krytycznych zdarzeniach bezpieczeństwa.

Analiza pojemności

Prognozy wzrostu i przewidywania “czasu do zapełnienia”, które zapobiegają kryzysom pojemności, zanim się wydarzą.

Raporty dla kadry zarządzającej

Raporty zgodności i gotowości do odtwarzania generowane jednym kliknięciem, gotowe dla kadry zarządzającej i audytorów — bez potrzeby arkuszy kalkulacyjnych.

5. Rezultaty

1. Pulpit operacyjny na żywo — widok statusu zadań, pojemności i bezpieczeństwa w czasie rzeczywistym.
2. Dziennik audytu śledczego — kompletna ścieżka audytu zmian konfiguracji i podejrzanych zachowań.
3. Raport analizy pojemności — prognoza wzrostu i przewidywanie “czasu do zapełnienia”.
4. Raporty zgodności & dla kadry zarządzającej — jedno kliknięcie, format gotowy do audytu.
5. Natychmiastowe alerty — przez integrację e-mail / webhook / SIEM.
6. Pulpit wielodostępny (multi-tenant) — odseparowany widok dla każdego klienta, dla dostawców MSP.

6. Zakres regulacyjny

Regulacja	Wymogi wspierane przez ZeroMON
BDDK	Art.45 backup, Art.51 wymóg ciągłego monitorowania, BT.31 wykrywanie ransomware
SPK III-35.1	Monitorowanie i raportowanie ciągłości działania
DORA (EU)	Art.11-12 monitorowanie polityki backupu, Art.17 dowody ciągłego testowania
KVKK	Art.12 środki techniczne — rejestrowanie dostępu & zmian
GDPR (EU)	Art.32 środki bezpieczeństwa — dowody ciągłego monitorowania
ISO 27001 / NIST	A.12.3 backup, A.12.4 rejestrowanie & monitorowanie, CSF DE (Detect)

7. Następny krok

Aby rozpocząć: BackupSec współpracuje z Tobą, aby zaplanować wdrożenie (OVA) oraz kroki połączenia tylko do odczytu, dzięki czemu ZeroMON zacznie działać w Twoim istniejącym środowisku Veeam w ciągu kilku minut.