ZeroMON

Platforma pro monitoring v reálném čase & zabezpečení pro Veeam backup infrastrukturu

“Vidět vše. Nepřehlédnout nic.” — Selhání odhalíte dříve, než přijde čas obnovy.

Služba	ZeroMON — Platforma pro observabilitu backupu
Zaměření	Monitoring Veeam Backup & Replication, bezpečnostní signály a kapacitní analytika
Verze	1.0
Datum	červen 2026
Pokrytí	BDDK · SPK · DORA · KVKK · GDPR · ISO 27001 · NIST
Poskytovatel	BackupSec

1. Co je ZeroMON?

ZeroMON je jednotná platforma pro observabilitu vaší backup infrastruktury: z jednoho místa monitoruje backup úlohy, bezpečnostní kontroly a přehled o prostředí Veeam. Je určen pro backup týmy, MSP a provozní týmy a odhaluje selhání, konfigurační drift a riziko obnovy po ransomwaru DŘÍVE, než přijde čas obnovy. ZeroMON je monitorovací vrstva rodiny BackupSec a doplňuje expertní poradenství ZeroTAM, penetrační testování ZeroPEN a cloudové úložiště ZeroVault.

> **Proč ZeroMON?** Každý backup systém vypadá v pořádku až do chvíle obnovy. ZeroMON zachytí neúspěšné úlohy, konfigurační drift, slabé kontroly immutability a falešnou jistotu — dříve, než se z nich stanou incidenty.

Čtyři vrstvy, nula kompromisů

ZeroMON funguje po boku zbytku rodiny BackupSec:

Služba	Role
ZeroMON	**Platforma pro observabilitu — monitoring v reálném čase a bezpečnostní signály (tento dokument)**
ZeroTAM	Expertní poradenství — architektura, kapacita, strategie a krizová podpora
ZeroPEN	Penetrační test & důkaz obnovy — testuje backupy tak, jak by to udělal útočník
ZeroVault	Cloudová storage služba — poslední kopie, kterou nelze smazat ani zašifrovat

Pro koho je určen?

- Backup týmy, které potřebují odhalit selhání, drift a riziko ransomwaru dříve, než přijde čas obnovy
- MSP a poskytovatele služeb spravující multi-tenant prostředí
- Provozní týmy provozující infrastrukturu založenou na Veeamu
- Auditní & bezpečnostní týmy, které chtějí compliance reporty na jedno kliknutí místo tabulek
- Organizace s povinnostmi dle BDDK / SPK / DORA / KVKK / GDPR

2. Katalog pokrytí monitoringu

ZeroMON průběžně monitoruje následující oblasti vašeho backup prostředí v reálném čase:

Oblast monitoringu	Obsah
Monitoring úloh & sledování SLA	Stav úspěchu/selhání backup/replikačních úloh, opakování, zpoždění a detekce porušení SLA
Monitoring repozitářů & kapacity	Míra zaplnění, trend růstu, prognóza “času do zaplnění”, výkon storage
Konfigurační drift & detekce změn	Sledování kdo/co/kdy u změn konfigurace úloh, repozitářů a oprávnění
Detekce bezpečnostních událostí	Podezřelé chování při mazání/šifrování, pokusy o neoprávněný přístup, upozornění založená na anomáliích
Stav immutability & hardeningu	Průběžné ověřování stavu Object Lock / hardened repozitáře, sledování období immutability
Stav komponent Veeam	Živý stav VBR serveru, proxy serverů, repozitářů a služeb Veeam
Multi-tenant pohled	Dashboard pro každého klienta, přístup na základě rolí a izolovaný reporting pro MSP
Compliance & manažerský reporting	Reporty compliance a připravenosti k obnově dle BDDK/SPK/DORA/KVKK/GDPR/ISO na jedno kliknutí
Integrace upozornění & notifikací	Okamžité směrování upozornění prostřednictvím e-mailu, webhooku a integrace se SIEM
Přístup pouze pro čtení & rezidence dat	On-premise nasazení, API přístup pouze pro čtení, data nikdy neopustí vaši síť (nulová exfiltrace dat)

3. Nasazení & životní cyklus

ZeroMON se nasazuje on-premise jako klient; nevyžaduje žádné změny ve vašem produkčním prostředí. Typický životní cyklus:

Fáze	Obsah
Nasazení	Stažení OVA klienta ze zákaznického panelu a jeho nasazení ve vlastním prostředí — bez nutnosti změn v produkci
Připojení	Připojení k vašim backup aplikacím pomocí uživatelského účtu pouze pro čtení
Baseline & kalibrace	Nastavení prahových hodnot a stanovení počátečního System Health Score
Živý monitoring (24/7)	Dashboard v reálném čase, okamžitá upozornění a forenzní logování
Pravidelný reporting	Reporty compliance & připravenosti k obnově připravené pro management a auditory

> **Závazek rezidence dat:** ZeroMON běží on-premise; backup data, telemetrie a konfigurační informace nikdy neopustí vaši síť. Připojení probíhají přes API přístup pouze pro čtení — nulová exfiltrace dat.

4. Klíčové funkce

Živý provozní dashboard

Sledování úloh v reálném čase, kalendářní pohledy a automatizované bezpečnostní kontroly backupu napříč celou vaší backup infrastrukturou.

Forenzní inteligence

Kompletní auditní stopy s okamžitými upozorněními na konfigurační změny, podezřelé chování a kritické bezpečnostní události.

Kapacitní analytika

Prognózy růstu a projekce “času do zaplnění”, které předcházejí kapacitním krizím dříve, než nastanou.

Manažerské reporty

Reporty compliance a připravenosti k obnově na jedno kliknutí, připravené pro management a auditory — bez nutnosti tabulek.

5. Výstupy

1. Živý provozní dashboard — pohled na stav úloh, kapacity a zabezpečení v reálném čase.
2. Forenzní auditní log — kompletní auditní stopa pro konfigurační změny a podezřelé chování.
3. Report kapacitní analytiky — prognóza růstu a projekce “času do zaplnění”.
4. Reporty compliance & manažerské reporty — jedno kliknutí, formát připravený pro audit.
5. Okamžitá upozornění — prostřednictvím e-mailu / webhooku / integrace se SIEM.
6. Multi-tenant dashboard — izolovaný pohled pro každého klienta pro MSP.

6. Regulatorní pokrytí

Regulace	Požadavky, které ZeroMON podporuje
BDDK	Art.45 backup, Art.51 očekávání průběžného monitoringu, BT.31 detekce ransomwaru
SPK III-35.1	Monitoring a reporting kontinuity provozu
DORA (EU)	Art.11-12 monitoring backup politiky, Art.17 průběžné doklady o testování
KVKK	Art.12 technická opatření — logování přístupů & změn
GDPR (EU)	Art.32 bezpečnostní opatření — doklady o průběžném monitoringu
ISO 27001 / NIST	A.12.3 backup, A.12.4 logování & monitoring, CSF DE (Detect)

7. Další krok

Jak začít: BackupSec s vámi naplánuje kroky nasazení (OVA) a připojení pouze pro čtení, aby byl ZeroMON ve vašem stávajícím prostředí Veeam v provozu během několika minut.