Rocket® software

Rocket® z/Assure® Continuous Vulnerability Monitor (CVM)

Continuous visibility into vulnerability exploitation and integrity risks on IBM Z®.

Introduction

Rocket® z/Assure® Continuous Vulnerability Monitor (CVM) helps organizations continuously monitor IBM Z® environments for exploitation activity and indicators of potential compromise. It complements scheduled vulnerability scans with continuous integrity monitoring.

CVM helps mainframe security and operations teams reduce exposure by continuously monitoring production environments for activity that could indicate vulnerability exploitation, authority escalation, or unsafe integrity conditions.

- **Continuous integrity monitoring:** Detects real-time exploit conditions and ability-to-exploit indicators as the environment changes.
- **Production-safe observation:** Monitors suspicious activity without injecting test cases or requiring an IPL.
- **VAP complement:** Extends point-in-time vulnerability analysis with continuous monitoring across production LPARs.
- **Dashboard-ready findings:** CVM streams findings to the dashboard for operational review and response.

By operationalizing continuous vulnerability monitoring, CVM helps teams shorten detection windows, strengthen operational resilience, and gain defensible visibility into evolving risk conditions across IBM Z environments.

CVM helps organizations address three critical challenges:

- Limited real-time visibility into IBM Z vulnerability exploitation conditions.
- Long detection windows between scheduled vulnerability scans.
- Manual detection processes and gaps in audit evidence for ongoing risk assessment.

Core Capabilities

CVM provides continuous visibility into vulnerability activity and integrity risk indicators, including:

- Real-time exploitation activity and ability-to-exploit conditions.
- Authority escalation indicators, including concerns identified through Accessor Environment Element (ACEE) analysis.
- System call behavior that may result in elevated authority.
- Suspicious integrity conditions such as first-read data overlays and memory handling issues.
- CVM started task alerts for operational monitoring.
- Rocket Security Portal dashboard streaming for finding review and response.

Key Benefits

01 Continuous integrity monitoring

CVM continuously monitors IBM Z environments for activity that may indicate exploitation or the ability to exploit integrity weaknesses.

Monitoring capabilities include:

- Detection of real-time exploit activity and ability-to-exploit indicators.
- Continuous evaluation of production environments without waiting for the next scheduled scan.
- Alerts on activities that violate integrity expectations.
- Streaming findings to support operational triage and risk response.

This gives teams a practical way to detect vulnerability activity as it happens instead of relying solely on periodic analysis.

02 Production-safe observation

CVM is designed to observe vulnerability-relevant behavior without disrupting production operations.

CVM monitors:

- Runtime behavior that may indicate exploitation activity or unsafe integrity conditions.
- Authority-related indicators, including conditions that may enable elevated access.
- Started task alerts and operational events that require security review.
- Findings streamed to the Rocket Security Portal for centralized review.

This approach helps teams continuously observe risk signals while minimizing operational disruption and accelerating investigation.

03 VAP complement for continuous monitoring

CVM complements z/Assure Vulnerability Analysis (VAP) by extending vulnerability management beyond scheduled assessments.

- Continuous VAP extension: VAP identifies vulnerability exposure at a point in time. CVM then monitors relevant activity during normal operations.
  - Shorter detection windows: Identifies risk-relevant activity between scheduled scans.
  - Operational prioritization: Helps teams focus on findings tied to active conditions.
  - Improved resilience: Supports faster investigation, validation, and response.
- Audit evidence consideration: Continuous monitoring findings can support risk review, incident investigation, and ongoing control validation. CVM helps teams understand not only where exposure exists, but also whether activity in the environment suggests that exposure requires immediate attention.

Operational reporting and response visibility

CVM delivers visibility in the formats teams need to support security operations, governance discussions, and vulnerability response workflows.

Outputs include:

- **Dashboard:** Centralized review of CVM findings and operational status.
- **Started task alerts:** Near-real-time indication of monitored activity that may require action.
- **Streaming output:** Integration-ready findings for downstream reporting and response workflows.
- **Operational summaries:** Executive-ready visibility into active risk indicators and response priorities.
- **CSV and PDF export:** Supports seamless data sharing, reporting, and offline analysis.
- **Real-time duplicate detection:** Identifies duplicate findings using confidence scoring ranging from 0% to 100%.
- **Analytics dashboard:** Provides daily trends, leading data sources, and key performance indicators (KPIs).
- **Detailed findings:** Technical evidence to support investigation, remediation, and control validation.

With CVM, organizations can strengthen mainframe vulnerability management by continuously monitoring exploitation activity, reducing detection gaps, and providing timely evidence for response and resilience.

Strengthen your mainframe vulnerability management program

Periodic scans establish a baseline. Continuous monitoring helps maintain it. With Rocket z/Assure Continuous Vulnerability Monitoring, your organization can move from reactive detection to continuous awareness, reducing detection windows, lowering manual burden, and building an evidence base that supports both operational response and long-term governance.

Learn more

About Rocket Software

Rocket Software is a global technology leader in modernization and a partner of choice that empowers the world's leading businesses on their modernization journeys, spanning core systems to the cloud. Trusted by over 12,500 customers and 750 partners, and with more than 3,200 global employees, Rocket Software enables customers to maximize their data, applications, and infrastructure to deliver critical services that power our modern world. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located throughout North America, Europe, Asia and Australia. Rocket Software is a portfolio company of Bain Capital Private Equity.

Talk to an expert

Rocket software

Modernization.
Without Disruption.™

Visit RocketSoftware.com

MAR-18875_Broch_CVMAssuranceLaunch_V4