Rocket® software

# Closing the Mainframe Vulnerability Gap

## Why prevention and continuous monitoring must work together

# Contents

# The mainframe security blind spot

Mainframes continue to run the most critical applications and data in the enterprise, yet many vulnerability management programs still treat them as an exception. Security leaders have invested heavily in cloud, endpoint, application, and infrastructure scanning, but the mainframe often remains outside the same continuous, evidence-based governance model.

That creates a strategic gap. Vulnerabilities can exist in compiled binaries, authorized programs, privileged execution paths, and production integrity conditions that conventional tools may not see. For organizations that rely on IBM Z® for revenue, payments, customer records, insurance processing, healthcare transactions, or regulated workloads, this isn't a technical issue alone. It's a business resilience, audit, and risk management issue.

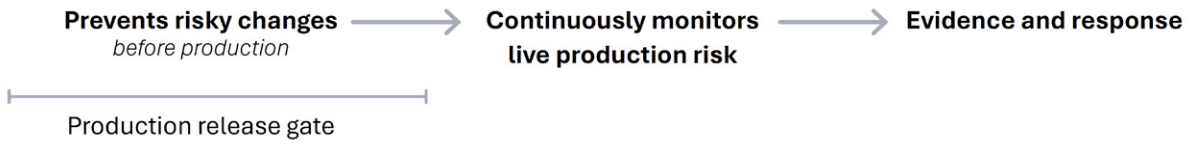
# A new executive mandate: prove mainframe risk is managed

Security executives are being asked a tougher question: can the organization prove that mainframe risk is being managed with the same discipline as the rest of the enterprise? The answer depends on more than periodic reviews or manual expertise. It requires a lifecycle approach that combines preventive assurance before change and continuous monitoring after systems are live.

Rocket z/Assure Vulnerability Analysis Program (VAP) and Rocket z/Assure Continuous Vulnerability Monitor (CVM) work together to address this mandate. VAP helps prevent vulnerable code and unvetted system changes from entering production. CVM helps maintain visibility into integrity and vulnerability-relevant activity once workloads are live.

**Continuous assurance that mainframe security controls are working is exactly what Rocket® z/Assurance™ and it's Rocket® z/Assure® products are built for.**

| Change Management / Pre-Production | Production Mainframe Environment | Evidence / Risk Reporting |
|---|---|---|
| Code Updates | IBM® Z Workloads | Audit Reports |
| Vendor Updates | Critical Applications | Governance Controls |
| System Changes | Sensitive Data | Executive Visibility |
| Privileged Routines | Privileged Execution Paths | |




# Why change management is the first line of defense

Every production change is a potential risk decision. New code, modified system software, vendor updates, authorized programs, and privileged routines can all introduce exposure if they're promoted without the right level of security validation. VAP brings deep vulnerability analysis into the change lifecycle, helping organizations identify code-based integrity issues before they reach production.

For buyers, this shifts mainframe security from reactive discovery to proactive threat reduction. VAP can support release governance, remediation validation, audit evidence, and risk-based approval. It gives security and operations teams a repeatable way to answer a critical question: should this change be allowed into production?

In a sales conversation, the value of VAP is not simply that it finds vulnerabilities. The value is that it helps organizations prevent avoidable exposure before it affects the business. It strengthens change control, reduces downstream remediation costs, improves audit confidence, and gives leaders a clearer line of sight between technical findings and business risk.

# Why production requires continuous visibility

Even the strongest release process cannot eliminate all risk. Production environments are dynamic. Workloads change, privileges evolve, operational conditions shift, and threat activity does not wait for the next scheduled assessment. CVM addresses this reality by continuously monitoring live environments for vulnerability-relevant activity, exploitation indicators, authority escalation concerns, and integrity risk conditions.

CVM gives security and operations leaders a way to reduce blind spots between periodic reviews. It observes production activity without forcing disruptive scan windows, helping teams identify emerging issues earlier, prioritize response, and demonstrate ongoing oversight of critical systems.

**This is the core message for customers:**

VAP helps keep risky changes out of production. CVM helps provide visibility into potential security threats after release. Together, they turn mainframe vulnerability management into a continuous assurance discipline.

# How security leaders can evaluate their approach

## Customer concern:

### 01 "How do we reduce mainframe risk before production?"

**VAP message:** Embed deep vulnerability analysis into change management and release approval.

**CVM message:** Use production monitoring to validate that risk conditions are not emerging after release.

### 02 "How do we prove controls are working?"

**VAP message:** Produce release-gate evidence that vulnerable code and privileged routines were assessed.

**CVM message:** Produce continuous monitoring evidence from live production environments.

## 03 “How do we reduce operational disruption?”

**VAP message:** Perform deep analysis in controlled pre-production or validation workflows.

**CVM message:** Observe production continuously without relying on disruptive scan windows

## 04 “How do we connect mainframe findings to business risk?”

**VAP message:** Prioritize vulnerabilities before promotion based on impact and exposure.

**CVM message:** Surface runtime indicators that require timely investigation and response.

# What continuous assurance enables for customers

- **Stronger governance:** Mainframe vulnerability management becomes part of release approval, production monitoring, and risk reporting.
- **Reduced exposure:** Risky code and privileged changes can be identified before they affect mission-critical systems.
- **Continuous assurance:** Production environments are monitored for vulnerability-relevant activity between periodic assessments.
- **Audit-ready evidence:** Teams can document both preventive and detective controls across the lifecycle.
- **Executive visibility:** Leaders gain a clearer view of mainframe risk in terms of business impact, operational resilience, and regulatory confidence.

## Why now?

Mainframes are central to enterprise resilience, but resilience cannot be assumed. Regulatory scrutiny, cyber risk, operational dependency, and executive accountability are converging. Organizations need to show that critical platforms are not only stable, but actively governed, monitored, and protected.

The organizations that modernize mainframe vulnerability management now will be better positioned to withstand audits, respond to threats, support digital transformation, and protect customer trust. VAP and CVM provide a practical path forward: integrate deep vulnerability analysis into change management and extend continuous monitoring into production.

# Gain confidence in the systems that run your business

Mainframe security can no longer be managed as a periodic, siloed, or exception-based activity. Organizations need a practical way to reduce mainframe risk before release and continuously monitor for emerging issues in production. VAP and CVM help meet that requirement with a lifecycle model that is defensible and aligned with enterprise security expectations.

**For security, risk, and operations leaders, the message is clear:**

prevent what you can before production, monitor what changes after release, and prove both with evidence the business can trust.

The next step is turning that strategy into practice.

**Speak to an expert**

## 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.

Rocket software

Modernization.
**Without Disruption.**™

Visit RocketSoftware.com



MAR-18971_WP_VAP_CVMThoughtLeadership_V3